

WILL TRANSPORTATION AND THE FAA BE READY FOR THE YEAR 2000?

JOINT HEARING
BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
OF THE
COMMITTEE ON GOVERNMENT REFORM
AND THE
SUBCOMMITTEE ON TECHNOLOGY
OF THE
COMMITTEE ON SCIENCE
HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTH CONGRESS
FIRST SESSION

MARCH 15, 1999

Committee on Government Reform

Serial No. 106-43

Committee on Science

Serial No. 106-46

Printed for the use of the Committee on Government Reform and the
Committee on Science



Available via the World Wide Web: <http://www.house.gov/reform>

U.S. GOVERNMENT PRINTING OFFICE

60-888 CC

WASHINGTON : 1999

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York	HENRY A. WAXMAN, California
CONSTANCE A. MORELLA, Maryland	TOM LANTOS, California
CHRISTOPHER SHAYS, Connecticut	ROBERT E. WISE, JR., West Virginia
ILEANA ROS-LEHTINEN, Florida	MAJOR R. OWENS, New York
JOHN M. McHUGH, New York	EDOLPHUS TOWNS, New York
STEPHEN HORN, California	PAUL E. KANJORSKI, Pennsylvania
JOHN L. MICA, Florida	PATSY T. MINK, Hawaii
THOMAS M. DAVIS, Virginia	CAROLYN B. MALONEY, New York
DAVID M. McINTOSH, Indiana	ELEANOR HOLMES NORTON, Washington,
MARK E. SOUDER, Indiana	DC
JOE SCARBOROUGH, Florida	CHAKA FATTAH, Pennsylvania
STEVEN C. LATOURETTE, Ohio	ELIJAH E. CUMMINGS, Maryland
MARSHALL "MARK" SANFORD, South	DENNIS J. KUCINICH, Ohio
Carolina	ROD R. BLAGOJEVICH, Illinois
BOB BARR, Georgia	DANNY K. DAVIS, Illinois
DAN MILLER, Florida	JOHN F. TIERNEY, Massachusetts
ASA HUTCHINSON, Arkansas	JIM TURNER, Texas
LEE TERRY, Nebraska	THOMAS H. ALLEN, Maine
JUDY BIGGERT, Illinois	HAROLD E. FORD, JR., Tennessee
GREG WALDEN, Oregon	_____
DOUG OSE, California	_____
PAUL RYAN, Wisconsin	BERNARD SANDERS, Vermont
JOHN T. DOOLITTLE, California	(Independent)
HELEN CHENOWETH, Idaho	

KEVIN BINGER, *Staff Director*

DANIEL R. MOLL, *Deputy Staff Director*

DAVID A. KASS, *Deputy Counsel and Parliamentarian*

CARLA J. MARTIN, *Chief Clerk*

PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois	JIM TURNER, Texas
THOMAS M. DAVIS, Virginia	PAUL E. KANJORSKI, Pennsylvania
GREG WALDEN, Oregon	MAJOR R. OWENS, New York
DOUG OSE, California	PATSY T. MINK, Hawaii
PAUL RYAN, Wisconsin	CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*

MATT RYAN, *Senior Policy Director*

MASON ALINGER, *Clerk*

FAITH WEISS, *Minority Counsel*

COMMITTEE ON SCIENCE

HON. F. JAMES SENSENBRENNER, JR., (R-Wisconsin), *Chairman*

SHERWOOD L. BOEHLERT, New York	GEORGE E. BROWN, JR., California, RMM**
LAMAR SMITH, Texas	RALPH M. HALL, Texas
CONSTANCE A. MORELLA, Maryland	BART GORDON, Tennessee
CURT WELDON, Pennsylvania	JERRY F. COSTELLO, Illinois
DANA ROHRABACHER, California	TIM ROEMER, Indiana
JOE BARTON, Texas	JAMES A. BARCIA, Michigan
KEN CALVERT, California	EDDIE BERNICE JOHNSON, Texas
NICK SMITH, Michigan	LYNN C. WOOLSEY, California
ROSCOE G. BARTLETT, Maryland	ALCEE L. HASTINGS, Florida
VERNON J. EHLERS, Michigan*	LYNN N. RIVERS, Michigan
DAVE WELDON, Florida	ZOE LOFGREN, California
GIL GUTKNECHT, Minnesota	MICHAEL F. DOYLE, Pennsylvania
THOMAS W. EWING, Illinois	SHEILA JACKSON-LEE, Texas
CHRIS CANNON, Utah	DEBBIE STABENOW, Michigan
KEVIN BRADY, Texas	BOB ETHERIDGE, North Carolina
MERRILL COOK, Utah	NICK LAMPSON, Texas
GEORGE R. NETHERCUTT, JR., Washington	JOHN B. LARSON, Connecticut
FRANK D. LUCAS, Oklahoma	MARK UDALL, Colorado
MARK GREEN, Wisconsin	DAVID WU, Oregon
STEVEN T. KUYKENDALL, California	ANTHONY D. WEINER, New York
GARY G. MILLER, California	MICHAEL E. CAPUANO, Massachusetts
JUDY BIGGERT, Illinois	VACANCY
MARSHALL "MARK" SANFORD, South Carolina	VACANCY
JACK METCALF, Washington	

SUBCOMMITTEE ON TECHNOLOGY

CONSTANCE A. MORELLA, Maryland, *Chairwoman*

CURT WELDON, Pennsylvania	JAMES A. BARCIA, Michigan**
ROSCOE G. BARTLETT, Maryland	LYNN N. RIVERS, Michigan
GIL GUTKNECHT, Minnesota*	DEBBIE STABENOW, Michigan
THOMAS W. EWING, Illinois	MARK UDALL, Colorado
CHRIS CANNON, Utah	DAVID WU, Oregon
KEVIN BRADY, Texas	ANTHONY D. WEINER, New York
MERRILL COOK, Utah	MICHAEL E. CAPUANO, Massachusetts
MARK GREEN, Wisconsin	BART GORDON, Tennessee
STEVEN T. KUYKENDALL, California	TIM ROEMER, Indiana
GARY G. MILLER, California	

EX OFFICIO

F. JAMES SENSENBRENNER, JR., Wisconsin+	GEORGE E. BROWN, JR., California+
---	-----------------------------------

CONTENTS

Hearing held on March 15, 1999	Page 1
Statement of:	
Willemssen, Joel C., Director, Civil Agencies Information Systems, General Accounting Office; Mortimer L. Downey, Deputy Secretary, Department of Transportation; Jane F. Garvey, Administrator, Federal Aviation Administration; and Kenneth M. Mead, Inspector General, Department of Transportation	8
Letters, statements, etc., submitted for the record by:	
Downey, Mortimer L., Deputy Secretary, Department of Transportation, prepared statement of	33
Garvey, Jane F., Administrator, Federal Aviation Administration, prepared statement of	39
Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statement of	3
Mead, Kenneth M., Inspector General, Department of Transportation: Letter dated May 20, 1999	79
Prepared statement of	52
Turner, Hon. Jim, a Representative in Congress from the State of Texas, prepared statement of	6
Willemssen, Joel C., Director, Civil Agencies Information Systems, General Accounting Office, prepared statement of	10

WILL TRANSPORTATION AND THE FAA BE READY FOR THE YEAR 2000?

TUESDAY, MARCH 15, 1999

HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY OF THE COMMITTEE ON GOVERNMENT REFORM, JOINT WITH THE SUBCOMMITTEE ON TECHNOLOGY OF THE COMMITTEE ON SCIENCE,

Washington, DC.

The subcommittees met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the Subcommittee on Government Management, Information, and Technology) presiding.

Present: Representatives Horn and Morella.

Staff present from the Subcommittee on Government Management, Information, and Technology: J. Russell George, staff director and chief counsel; Matt Ryan, senior policy director; Bonnie Heald, director of communications; Mason Alinger, clerk; Faith Weiss, minority counsel, Committee on Government Reform; and Jean Gosa, minority staff assistant, Committee on Government Reform.

Staff present from the Subcommittee on Technology: Jeff Grove, staff director; Ben Wu, professional staff member; and Joe Sullivan, clerk.

Mr. HORN. A quorum being present, I call this joint hearing of the House Subcommittee on Government Management, Information, and Technology, and Subcommittee on Technology to order.

Each year more than 500 million passengers board airplanes. Most of them are secure in the knowledge that they will reach their destination safely and reasonably on time. They depend on the intricate computers that keep the network of communications and mechanical systems running—whether the year is 1999 or 2000.

But that's only one part of the Nation's vital transportation infrastructure. The railroads are an equally integral part of the travel and commerce that support everyday life in America.

Each year, thousands of lumbering freight trains move across the Nation's network of rail lines, carrying millions of tons of goods and raw materials. These are the items that keep our store shelves filled and our factories open. The railroads remain one of the most vital links to the continued prosperity of this country.

The port of Long Beach, which is in my district, is the busiest container port in the United States, sixth busiest in the world. In 1997, nearly 60 million metric tons of cargo moved through the port, everything from petroleum, iron, and steel, to electronics,

toys, and motor vehicles. Fifty percent of these imports are moved by train to cities in the Midwest and East.

We must make sure that neither of these vital networks falls victim to the year 2000 computer problem.

The challenge, often called the "Millennium Bug" or simply "Y2K," dates back to the 1960's and 1970's when computers were bulky in size but small in memory. To conserve limited space, or memory, programmers began designating the year by using two digits rather than four. The year 1967, for example, appears as "67." The first two digits are assumed to be "19."

Unless corrected, these data-sensitive computer systems and microchips, embedded in countless mechanical devices, may misinterpret the two zeros in 2000 as 1900. The fear is that this confusion may cause the systems to generate erroneous information, corrupt other systems, or possibly shut down.

In February the Department of Transportation, which is responsible for overseeing the Nation's air and rail lines as well as Federal highways and waterways, reported that only 53 percent of its mission-critical computer systems are year 2000 compliant.

At the same time, the Federal Aviation Administration, which oversees air safety and operates the Nation's vital air traffic control system, reported that only 60 percent of its mission-critical systems were ready for January 1, 2000.

The FAA has said it cannot meet President Clinton's March 31st deadline to be 100 percent compliant. But will the agency be able to meet its own self-imposed deadline of June 30, 1999?

To its credit, the FAA has historically maintained one of the finest safety records in the world, and we have no doubt that everyone at this agency is working extremely hard to retain that highly regarded status.

We are here today to learn how the enormous year 2000 challenge is being met—in the air, on the ground, and on the Nation's waterways.

[The prepared statement of Hon. Stephen Horn follows:]

DAN BURTON, INDIANA
CHAIRMAN
BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MOWELL, MARYLAND
CHRISTOPHER DAVIS, CONNECTICUT
KLEA ROS LEHTINEN, FLORIDA
JOHN M. REAGAN, NEW YORK
STEVEN HORV, CALIFORNIA
NICK FLORES
JAS. M. DAVIS, VIRGINIA
DAVID M. MCINTOSH, INDIANA
NORM E. SCHUBER, INDIANA
JOE SCARBOROUGH, FLORIDA
STEVEN L. TONNETTE, OHIO
MARSHALL "MARK" SANFORD, SOUTH CAROLINA
BOBBIE GEORGE
DAN MILLER, FLORIDA
ASA HUTCHINGS, ARKANSAS
LEE TERRY, NEBRASKA
JUDY BIGGERT, ILLINOIS
ORIG WALDEN, OREGON
DOUGLASE, CALIFORNIA
PAUL RYAN, WISCONSIN
JOHN T. DODDLETT, CALIFORNIA
HELEN CHENOWETH, IDAHO

ONE HUNDRED SIXTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

MAJORITY : (202) 225-5074
MINORITY : (202) 225-3551
TTY : (202) 225-6852

HENRY A. WILMAN, CALIFORNIA
RANKING MEMBER
TOM LANTOS, CALIFORNIA
ROBERT E. WISE, JR., WEST VIRGINIA
MAJOR R. OWENS, NEW YORK
EDWIN W. TOWNE, NEW YORK
PAUL E. KANARSKI, PENNSYLVANIA
GARY A. COSSETT, CALIFORNIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELIZABETH HOLMES, MONTANA
DISTRICT OF COLUMBIA
CHARAK FATTAH, PENNSYLVANIA
ELIZABETH CHAMBERS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BEAGLE, ILLINOIS
DANIEL K. DAVIS, ILLINOIS
JOHN P. TERRY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
HAROLD E. FORD, JR., TENNESSEE

BERNARD SANDERS, VERMONT,
INDEPENDENT

**"Will the FAA and the Department of Transportation
be ready for the Year 2000?"**

CHAIRMAN STEPHEN HORN
OPENING STATEMENT
March 15, 1999

A quorum being present, I call this joint hearing of the House Subcommittee on Government Management, Information, and Technology and the Subcommittee on Technology to order.

Each year, more than 500 million passengers board airplanes. Most of them are secure in the knowledge that they will reach their destination safely and reasonably on time. They depend on the intricate computers that keep the network of communications and mechanical systems running -- whether the year is 1999 or 2000.

But that's only one part of the nation's vital transportation infrastructure. The railroads are an equally integral part of the travel and commerce that support everyday life in America.

Each year, thousands of lumbering freight trains move across the nation's network of rail lines, carrying millions of tons in goods and raw materials. These are the items that keep our store shelves filled and our factories open.

The railroads remain one of the most vital links to the continued prosperity of this country.

✦ The Port of Long Beach, which is in my district, is the busiest container port in the United States, sixth busiest in the world. In 1997, nearly 60 million metric tons of cargo moved through the port -- everything from petroleum, iron and steel to electronics, toys and motor vehicles. Fifty (50) percent of those imports are moved by train to cities in the Midwest and East.

✦ We must make sure that neither of these vital networks falls victim to the Year 2000 computer problem.

The challenge, often called the "Millennium Bug" or simply "Y2K," dates back to the 1960s and 1970s when computers were bulky in size but small in memory. To conserve limited space, or memory, programmers began designating the year by using two digits rather than four. The year "1967," for example, appears as "67." The first two digits are assumed to be "19."

Unless corrected, these date-sensitive computer systems and microchips, embedded in countless mechanical devices, may misinterpret the two zeros in "2000" as "1900." The fear is that this confusion may cause the systems to generate erroneous information, corrupt other systems or possibly shut down.

In February, the Department of Transportation, which is responsible for overseeing the nation's air and rail lines as well as federal highways and waterways, reported that only 53 percent of its mission-critical computer systems are Year 2000 compliant.

At the same time, the Federal Aviation Administration, which oversees air safety and operates the nation's vital air traffic control system, reported that only 60 percent of its mission-critical systems were ready for January 1st, 2000.

Mr. HORN. I welcome today's witnesses and look forward to their testimony. We have a good part of the leadership of the Department of Transportation, with Deputy Secretary Mortimer Downey, Administrator of the Federal Aviation Administration Jane Garvey.

We will start with our first witness, which is the representative of the General Accounting Office which is the Congress's programmatic and fiscal auditor. We try to send them into every agency. And so we welcome Joel Willemssen, Director, Civil Agencies Information Systems, GAO, part of the legislative branch, and Mr. Kenneth M. Mead, Inspector General, Department of Transportation.

As you all know, we swear in all witnesses before this subcommittee, and I would ask you if some of your assistants are going to contribute to the dialog, I would just as soon swear in everybody now. That is what I did with the Department of Defense on another subject, and that saves me giving oaths. So if all will stand up, please raise your right hands.

[Witnesses sworn.]

Mr. HORN. I note that there are roughly 10 or 11 that affirmed that oath.

And so we will begin with Mr. Willemssen—

Mrs. MORELLA. Would you like me to make an opening statement?

Mr. HORN. Sure. I didn't see you come in.

Mrs. MORELLA. I am so small.

Mr. HORN. The distinguished co-chairman of the working group, task force, on the House side, but more important, chairman of the Subcommittee on Technology of the House Committee on Science.

Mrs. MORELLA. Thank you, Mr. Chairman. I am pleased to be here as chairman of the House Science Committee's Technology Subcommittee. I am pleased to join the Committee on Government Reform's Government Management, Information, and Technology Subcommittee in this important hearing to explore the impact of the year 2000 computer problem upon critical components of our Nation's transportation system.

Our transportation system consists of many interlocking components, supported by a complicated aviation infrastructure and 5.5 million miles of public roads, rail track, waterways and pipelines. Over the years, advanced technologies and computers have been implemented by the transportation sector to improve efficiency.

Inadvertently, its reliance on technology also exposes the transportation sector to significant Y2K risks. Clearly transportation and the movement of people and goods is absolutely vital to our Nation. We simply cannot afford to allow the mobility of our society to be disrupted by the millennium bug.

The Office of Management and Budget, the General Accounting Office and the Inspector General, as well as the Congress, have been very critical of the Department of Transportation's Y2K efforts to date. Most of the criticism is due to the fact that the Department and the FAA did not begin to seriously address the extent of the year 2000 problem until February 1998, much too late.

For its part, I must say that the Federal Aviation Administration under the leadership of Administrator Jane Garvey has been very forthright in recognizing its mistakes of the past. I am pleased to

commend Administrator Garvey and the agency for the remarkable progress it has made in the last year. However, the job is not finished. There is still much work to do.

Currently the FAA has implemented Y2K changes in roughly one-third of its air traffic control systems at its field sites. The remaining two-thirds are more complex and have to be installed at 3,000 different locations over the next 3 months. In addition to making sure that their own internal systems work, the FAA has also got to coordinate its efforts with airports, international organizations and other Federal agencies.

There is still much to do and a very short amount of time to ensure that the right Y2K solutions are put into place. While I have confidence in their leadership, I am convinced that it is critical for the Department and the FAA to work proactively with all transportation stakeholders in the development of contingency plans that ensure that the transportation of people, goods and services are not significantly impaired on January 1, 2000 and beyond.

So I am pleased that today we have a very distinguished panel of witnesses before us. I look forward to their comments, their recommendations. The fact that this is the fourth hearing we have held on transportation and year 2000 underscores its importance to our subcommittees and to our Nation. We all share the same goal of a seamless transition to the year 2000. The American people expect no less.

Thank you, Mr. Chairman.

Mr. HORN. Thank you very much, and without objection, the opening statement of the ranking minority member, Mr. Turner of Texas, will be put in the record at this point.

[The prepared statement of Hon. Jim Turner follows:]

STATEMENT OF THE HONORABLE JIM TURNER
JOINT HEARING "WILL TRANSPORTATION AND FAA BE READY FOR
THE YEAR 2000?"

March 15, 1999

I am glad to join Chairman Horn and Chairwoman Morella to discuss the status of Year 2000 (or "Y2K") readiness at the Department of Transportation. I would like to welcome the Deputy Secretary of Transportation, Mr. Downey; the Administrator of the FAA, Ms. Garvey; the Transportation Department's Inspector General's office; and the General Accounting Office, and thank everyone here today for their hard work and effort.

The Transportation Department's most recent Y2K report indicates that the Federal Aviation Administration and the US Coast Guard are behind in their Y2K conversion efforts. However, there has been serious and sustained attention at the highest levels of the Department of Transportation and the FAA, and we are beginning to see the results.

The FAA has made substantial progress since November, and agency reports that it has finished repair work on 74 % of its mission-critical systems; which is up from only 20 % reported in November. The FAA and those who have worked to turn the Y2K program around from where it was last February deserve great credit. However, the FAA does still face potential turbulence ahead as the agency, over the next three months, rolls out about 4,000 individual repairs to systems which are located at as many as 600 different facilities nationwide.

The FAA must also work closely with the airlines, airports, and air traffic controllers to assure that the business continuity and contingency plans of all those involved form a seamless safety net. Additionally, we need to get the best information on international readiness out to American travelers as soon as it becomes available, and I am pleased to hear that the FAA and the Departments of Transportation and State are planning to release recommendations for foreign travel by September 30, 1999.

Furthermore, the Administration's Y2K Council has expressed concern with the Y2K awareness and preparation of the international shipping industry. Given this concern, I am pleased to learn that the United States Coast Guard, in partnership with the International Maritime Organization, is actively addressing the Y2K readiness of the global maritime industry.

Moreover, the Transportation Working Group of the Y2K Council noted in its first sector assessment of the transportation industry that "the potential readiness of airports and transit services in small communities and rural areas is a concern." Because I represent a rural district, I would be interested in knowing what can be done at the federal level to assure that rural transportation issues are addressed and that Y2K won't disproportionately affect or burden small or rural towns.

Mr. HORN. We now begin with our first witness, Mr. Joel Willemssen, the Director of Civil Agencies Information Systems of the General Accounting Office. Mr. Willemssen.

STATEMENTS OF JOEL C. WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, GENERAL ACCOUNTING OFFICE; MORTIMER L. DOWNEY, DEPUTY SECRETARY, DEPARTMENT OF TRANSPORTATION; JANE F. GARVEY, ADMINISTRATOR, FEDERAL AVIATION ADMINISTRATION; AND KENNETH M. MEAD, INSPECTOR GENERAL, DEPARTMENT OF TRANSPORTATION

Mr. WILLEMSSEN. Thank you, Mr. Chairman, Chairwoman Morella, and thank you for inviting GAO to testify today on DOT's Y2K readiness. As requested, I will briefly summarize our statement and in particular focus on the Y2K readiness of the Federal Aviation Administration.

Over the past year FAA has made tremendous progress on Y2K. After a very slow start, FAA now has a strong management structure, an overall Y2K strategy, detailed standards and guidance, schedules and milestones for key activities, and a draft business continuity and contingency plan. Despite this progress, FAA still has a long way to go. Trying to play catch-up after such a slow start, especially given the complexity of FAA's systems and environment, is an enormous undertaking.

For example, many of FAA's mission-critical systems are not due to be implemented until after OMB's deadline this month. Several of these are among FAA's most critical systems. FAA also faces the challenge of making sure that validation of systems is sufficient and complete. In reviewing reports and test documentation for a sample of six mission-critical air traffic systems, we found that validation of three was supported. However, we found one other system's testing to be insufficient, and two systems lacked supporting documentation to determine whether testing was adequate.

For example, for the automated radar terminal or ARTS-III, system which provides aircraft position and flight plan information to controllers, FAA's validation may have been premature. This system continues to rely on a 1960's vintage computer. Home computers available today have 250 times the memory of this computer.

Ten years ago we reported on the flight safety risks associated with this old computer and recommended to FAA that it pursue alternatives to replace the system. However, this computer is still used by air traffic controllers at over 50 locations. In looking at this system for Y2K compliance, we found shortcomings in the analysis of the software, testing, and the contractors' determination of compliance.

FAA faces other challenges. It still needs to deploy about 75 systems to hundreds of air traffic facilities. Concurrently rolling out numerous system changes to multiple sites will be time-consuming and resource-intensive, and FAA has acknowledged that schedules are tight—with no room for delay.

Data exchanges represent another major challenge for FAA. It reports more than 1,000 in its inventory and more than 100 requiring modification, and we are continuing to review FAA's progress

in this area. In-depth testing of multiple systems that have individually been deemed compliant is another key activity. FAA has made progress on this since our last testimony and now has developed detailed end-to-end test plans that we are continuing to review.

In addition to the risks of its internal systems, FAA is also at risk that external systems will fail. For example, we recently reported on airports' efforts to address Y2K. Of the 234 airports responding to our surveys, about one-third reported that they would complete their preparations by June 30th. The other two-thirds planned on a later completion date or did not have an estimated completion date, and half of these did not have contingency plans for any of their core business functions.

Because of the risk of system failures, whether from internal systems or reliance on external partners and suppliers, FAA needs a comprehensive business continuity and contingency plan to help ensure continuing operations. FAA has drafted such a plan and intends to release four more iterations of this plan throughout the year.

That concludes a summary of my statement, and I would be pleased to address any questions you may have.

[The prepared statement of Mr. Willemsen follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management,
Information and Technology, Committee on Government
Reform, and the Subcommittee on Technology, Committee on
Science, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Monday,
March 15, 1999

YEAR 2000 COMPUTING CRISIS

FAA Is Making Progress But Important Challenges Remain

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division



Mr. Chairman, Ms. Chairwoman, and Members of the Subcommittees:

We appreciate the opportunity to testify on the Federal Aviation Administration's (FAA) efforts to address the Year 2000 problem. With fewer than 300 days remaining until January 1, 2000, this critical issue is at the forefront of the world's information technology challenges, and is especially crucial to FAA.

Hundreds of critical computer systems make FAA's operations possible. FAA uses these systems to effectively control air traffic, target airlines for inspection, and provide up-to-date weather conditions to pilots and air traffic controllers. However, many of these systems could fail to perform as needed when using dates after 1999 unless proper date-related calculations can be ensured. Should systems fail or malfunction, hundreds of thousands of people could be affected through customer inconvenience, increased airline costs, grounded or delayed flights, or degraded levels of safety.

My statement today will focus on five topics: (1) FAA's progress to date, (2) the agency's self-reported data showing that much remains to be done, (3) challenges FAA faces in ensuring its internal systems will work, (4) risks associated with external organizations—focusing specifically on airports and international entities, and (5) the critical need for business continuity and contingency plans that identify how aviation operations will continue should systems fail.

In brief, FAA and its employees have worked hard over these past months and continue to show dedication in tackling the monumental Year 2000 problem. Looking back to where the agency

was only a year ago, FAA has made tremendous progress. However, much remains to be done to complete validating and implementing FAA's mission-critical systems, and the agency continues to face challenges in making these internal systems Year 2000 compliant. Additionally, the risk of failures by external organizations, such as airports and foreign air traffic control systems, could seriously affect FAA's ability to provide aviation services—which could have a dramatic effect on the flow of air traffic across the nation and around the world. To mitigate the risk that critical internal or external systems will fail, FAA needs sound business continuity and contingency plans.

FAA Has Made Substantial Progress In Its Year 2000 Program

Over the past year, FAA has made substantial progress. In January 1998 FAA had no central Year 2000 program management; an incomplete inventory of mission-critical systems; no overall strategy for renovating, validating, and implementing mission-critical systems; and no milestone dates or schedules. At that time, we recommended that FAA provide its Year 2000 program manager with the authority to enforce policies; outline FAA's overall strategy for addressing the Year 2000 date change; complete inventories of all information systems and interfaces; set priorities; establish plans for renovating, validating, and testing all converted and replaced systems; and develop Year 2000 business continuity and contingency plans to ensure the continuity of critical operations.

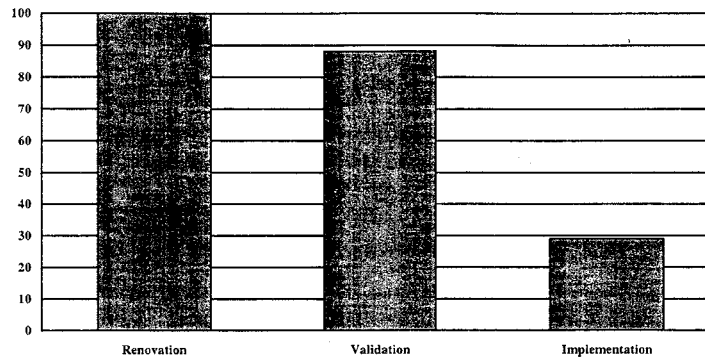
FAA has now addressed these recommendations. The agency has a strong Year 2000 management structure; an overall Year 2000 strategy; detailed standards and guidance for renovating, validating, and implementing mission-critical systems; a database of schedules and

milestones for these activities; and a draft Year 2000 business continuity and contingency plan. Additionally, FAA reported that it completed 99 percent of its mission-critical systems repairs by the Office of Management and Budget's (OMB) September 1998 deadline, and 74 percent of its systems testing by OMB's January 1999 deadline.

Self-Reported Data Show FAA Still Has Much To Do

While the government-wide deadline for completing systems implementation is at the end of this month, FAA's self-reported data demonstrate that much work remains to be done in a limited amount of time. Specifically, FAA must still finish implementing 141 mission-critical systems. Figure 1 details the overall reported status of FAA's mission-critical systems as of March 8, 1999.

Figure 1: Percentage of Mission-Critical Systems That Have Completed Key Year 2000 Phases as of March 8, 1999.



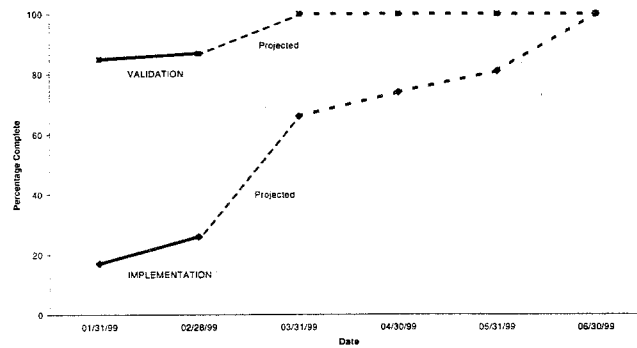
Source: FAA.

As of March 8, 1999, FAA's internal systems database showed that 50 of its 423 mission-critical systems had not yet been validated. These include 25 systems that have been repaired, 5 replacement systems, and 20 systems that were determined not to need repair or replacement. FAA intends to complete validation of all mission-critical systems by March 31, 1999.

Much more remains to be done to complete the implementation of mission-critical system repairs and replacements. While FAA determined that 224 of its 423 mission-critical systems do not require changes to be made, the remaining 199 systems (47 percent) must be modified, replaced, or newly installed. As of March 8, 1999, FAA reported that it had implemented 58 of these 199 systems. The agency plans to implement an additional 74 systems by March 31, and the

remaining 67 systems by June 30, 1999. Figure 2 details FAA's schedule for completing the validation and implementation of its mission-critical systems.

Figure 2: Percentage of Mission-Critical Systems Completing Validation and Implementation Over Time



Source: FAA.

Many Critical Air Traffic Control Systems

Still Await Validation and Implementation

FAA has identified 26 mission critical systems as posing the greatest risk to the National Airspace System (NAS)—the network of equipment, facilities, and information that supports U.S. aviation operations--should their repairs experience schedule delays or should the systems not be operational on January 1, 2000. FAA ranked mission-critical air traffic control systems based on their impact and criticality to the NAS, their overall functionality, and an evaluation of the risk associated with solving the Year 2000 problem.

As of March 8, 1999, five of these critical systems had not yet been validated, and 14 had not yet been implemented. Twelve of the 14 that have not yet been implemented—providing critical functions ranging from communications to radar processing to weather surveillance—are not scheduled to be implemented until after March 31, 1999.¹

FAA's Year 2000 Efforts Face Significant Challenges

FAA faces several challenges in completing its Year 2000 activities. These challenges include

- ensuring that systems validation efforts are adequate,
- implementing multiple systems at numerous facilities,
- completing data exchange efforts, and
- completing end-to-end testing.

¹ The 12 systems include (1) the Automated Radar Terminal System (ARTS-III-E); (2) the Host Environment; (3) the En Route Automated Radar Tracking System (EARTS); (4) the Graphic Weather Display System (GWDS); (5) the U.S. Notices to Airmen System (US NOTAMS); (6) the Aeronautical Mobile Communications Services (AMCS); (7) the Integrated Communications Switching System (ICSS) Litton-types 2 and 3; (8) ICSS type III-Denro; (9) Terminal Doppler Weather Radar (TDWR); (10) the Remote Maintenance Monitoring System (RMMS); (11) Heating, Ventilation and Air Conditioning (HVAC) Systems; and (12) Mejoras Al Enlace De Voz Del ATS (MEVA), a satellite-based communications system in the Caribbean and Central American regions.

Support for Systems' Validation Is Not Always Sufficient and Complete

FAA's Year 2000 program office has developed standards for testing and implementing mission-critical systems that require system owners to prepare and obtain approval on a validation plan that includes test plans and procedures, funding requirements, test management roles, and schedules. The system owners are then required to test the system according to this plan, complete a checklist of required validation activities, and prepare a Year 2000 validation results report. Once this report has been approved within the relevant FAA business line, a contractor for FAA's Year 2000 program office performs an independent verification and validation (IV&V) review of key validation documents. The system is then considered ready to be implemented.

In reviewing validation plans, reports, and supporting test documentation for six mission-critical air traffic systems² that were reported as having completed validation, we found that the validation of three systems was supported.³ However, one system's testing was found to be insufficient, and two systems lacked the documentation necessary to ensure that testing was adequate.

² In choosing systems for our case studies, we attempted to cover a range of air traffic control functions in different environments. We selected validated systems from three different critical core functions (surveillance, communications, and weather processing) that operated in one or more of the different air traffic control environments (en route, terminal, tower, and flight service station). Two of the systems (FSAS and ICSS-Litton type 2.3) were also chosen because they were identified by FAA as among the 26 most at-risk systems.

³ These systems are the Voice Switching and Control System (VSCS), the Display System Replacement (DSR), and the Low Level Windshear Alert System (LLWAS) version FA-10240.

ARTS-III Validation Testing Is Insufficient

The Automated Radar Terminal System (ARTS)-III is the critical data processing system used in about 55 terminal radar approach control facilities. These systems provide essential aircraft position and flight plan information to controllers. The ARTS-III system continues to rely on a 1960s-vintage computer (a UNIVAC 8303 Input Output Processor), which was originally produced by UNIVAC but is now supported by the Lockheed Martin Corporation. Home computers available today have 250 times the memory of this archaic processor. In 1989 and 1990 we reported on the flight safety risks associated with this system, and recommended that FAA assess other alternatives for meeting air traffic requirements.⁴ However, FAA did not act on our recommendation, stating that it had a plan—which included continuing with the old processors. Ten years later, these processors are still in operation.

FAA validated the ARTS-III system based on source code analysis, testing, and vendor inquiries performed by Lockheed Martin, whose representatives told us that they retained some of the experts who had worked on the UNIVAC 8303 processor in the 1960s. Source code analysis was used to identify all data processing code in the system. Testing was performed after problematic code was repaired, and vendor inquiries were used to determine the Year 2000-compliance status of all commercial-off-the-shelf (COTS) hardware, firmware, and software in the ARTS-III system. Because of its criticality, we focused on the ARTS-III subsystem that uses the UNIVAC 8303 processor and processes radar data. We found shortcomings in the

⁴ Air Traffic Control: Computer Capacity Shortfalls May Impair Flight Safety (GAO/IMTEC-89-63, July 6, 1989) and Air Traffic Control: Inadequate Planning Increases Risk of Computer Failures in Los Angeles (GAO/IMTEC-90-49, July 16, 1990).

source code analysis, testing, and vendor assessment of the UNIVAC processor, which form the basis for FAA's decision to validate this system.

Specifically, the analysis of the ARTS-III source code, which includes code written in UNIVAC Ultra assembly language, depended upon using a common text search utility to search for ten specific character strings that included "DECADE," "LEAP," "YEAR," "DATE," and "DAY." However, computer programs written in assembly language do not use only common English words such as "YEAR" and "DATE" for names of date fields. Instead, assembly language programs often use cryptic names such as DATCHK (for "date check") or CURDAT (for "current date"). Thus, FAA's analysis may not have found all date processing code in the Ultra assembly language programs that run in the UNIVAC processor. FAA officials stated that the code analysis was sufficient because they believe there are no date-related items in the code. We believe that the criticality of this system warrants a more thorough analysis.

The ARTS-III system testing consisted of two phases. The first phase, performed at FAA's Technical Center, involved evaluating data file transfers between the ARTS-III memory and the peripheral equipment during simulations rolling the date forward through key dates—including from December 31, 1999 to January 1, 2000. The second phase, key site testing, involves performing Year 2000-rollover and functional evaluations at a site. FAA's test documentation showed that these tests focused primarily on off-line programs, such as an editing application. The test documentation does not show any tests designed to validate the radar tracking functionality of the UNIVAC 8303 Input Output Processor at critical dates. Therefore, FAA's testing to date validated data exchanges between the ARTS-III memory and the peripheral

devices in Year 2000, but not the critical functionality of tracking real radar data. FAA officials responded that they did not test the radar tracking functions because they did not make any modifications to these applications. However, the Lockheed Martin's test report showed that there are date calculations in operational segments of the ARTS-III system. Therefore FAA should test these functions. FAA officials stated that they plan to test the radar tracking functions during end-to-end testing.

Further, FAA's use of vendor inquiries to assure the Y2K compliance of COTS hardware, firmware, and software was insufficient, given the criticality of the ARTS-III system. The list of COTS hardware includes the UNIVAC 8303 input-output processor, which is no longer produced. FAA officials told us that they did not request or obtain a statement from the manufacturer that the processor was Year 2000 compliant. Instead, FAA relied on Lockheed Martin's finding--based on analysis by an engineer that had worked on the UNIVAC processor since the 1960s--that there were no Year 2000 issues associated with the processor. Given the criticality of this processor, FAA's Year 2000 program manager agreed that a statement of the processor's Year 2000 compliance would be nice to have. A Lockheed Martin representative agreed to look into the possibility of providing such a statement.

Because of shortcomings in the source code analysis, testing, and vendor certification of the UNIVAC processor's Year 2000 compliance, FAA's validation of the ARTS-III system may be premature. A statement from the vendor that the UNIVAC 8303 processor is Year 2000 compliant together with FAA's planned end-to-end testing of radar tracking functions should

provide greater assurance that the system will work through the Year 2000 date change as anticipated.

Two Systems' Tests Lack Supporting Documentation

The Integrated Communications Switching System (ICSS)⁵ supports ground-to-ground voice communications between air traffic controllers in adjacent facilities and air-to-ground voice communications between air traffic controllers and pilots. We reviewed ICSS test results and found that they lacked sufficient details to determine if all required testing was actually conducted. Specifically, for 1 of 2 key components, we could not determine whether required tests for processing 5 of 11 critical dates had been performed and passed.⁶ If they were not tested, the risk that the system could experience unanticipated failures on these specific dates is increased. FAA testing documents also did not specify which version of ICSS had been tested and deemed Year 2000 compliant. As a result, the version of ICSS that was successfully tested may not be the version that is implemented in air traffic control facilities. If it is not, there is an increased risk of Year 2000-induced communications failures between air traffic controllers.

The test results for the Flight Service Automation System (FSAS), which provides essential weather information and flight planning services to general aviation pilots, also did not show whether the required tests for processing 6 of the 11 critical dates had been performed and

⁵ There are multiple versions of ICSS in FAA's mission-critical systems inventory. We reviewed the validation information on ICSS-Litton types 2 and 3.

⁶ FAA's compliance checklist requires the following 11 dates to be checked to ensure that they roll over to the next day correctly: 12/31/1998, 9/9/1999, 9/30/1999, 12/31/1999, 1/1/2000, 2/28/2000, 2/29/2000, 3/1/2000, 12/31/2000, 1/1/2001, and 12/31/2027.

passed. As a result, to the extent that the tests were not performed, FSAS is also at risk of failing unexpectedly on these dates, potentially affecting the flight planning capabilities of the general aviation community—a group that comprises over 95 percent of all flights within the United States. In responding to a draft of this testimony late last week, an FAA official stated that he was confident that all of the dates had been tested, and agreed to provide the supporting documents this week.

Further, the validation plans for both ICSS and FSAS were not completed prior to testing, in accordance with FAA standards. For example, FAA conducted FSAS validation testing through June 1998, but the plan for conducting the validation test was written in July 1998. Not having a plan before testing compromises the integrity and objectivity of the tests and raises the risk that critical testing will be overlooked.

The Number of FAA Air Traffic Control Facilities Complicates Systems Implementation

FAA's ability to implement system repairs and replacements in a timely manner is complicated by the agency's highly decentralized nationwide configuration of air traffic control facilities.

FAA intends to deploy about 75 mission-critical air traffic control systems to one or more of its roughly 654 air traffic facilities.⁷ Concurrently rolling out numerous systems changes to multiple

⁷ These facilities include the Air Traffic Control System Command Center, Automated Flight Service Stations, Flight Service Stations, Alaskan Rotational Flight Service Stations, Air Route Traffic Control Centers, Airport Traffic Control Towers, Terminal Radar Approach Control facilities, Radar Approach Control facilities, and Combined Center/Radar Approach Control facilities.

sites will be time-consuming, labor-intensive, and filled with difficult implementation challenges.

FAA's Year 2000 program manager acknowledged that schedules are tight and there is no room for any schedule delays. He estimated that FAA has to complete roughly 4500 "events" by June 30, 1999—each one entailing the activation of a single system in a single site. To aid in this monumental task, FAA has established system implementation schedules for managing system changes at its facilities.

Data Exchange Efforts Are Ongoing

In order to ensure that systems will successfully navigate the Year 2000 date change, systems' data exchanges must be assessed and any necessary modifications must be made. If not addressed, data exchanges could cause the failure of an otherwise compliant system.

Last month, FAA reported that it had 1,127 data exchanges in its inventory. After evaluating each, the agency determined that 119 data exchanges required modification. FAA reports that these data exchanges are associated with 42 different systems. As of last week, 33 of these systems have been validated and 12 have been implemented. FAA plans to complete implementing modifications to the data exchanges on its mission-critical systems by June 30, 1999.

While most of these systems' data exchanges requiring modification are between internal FAA systems, ten systems also exchange data with outside entities. Specifically, three systems

exchange data with other federal agencies, such as the National Aeronautics and Space Administration and the National Transportation Safety Board, three exchange data with other entities, such as foreign air traffic control providers, and two systems exchange data with both other federal agencies and other entities. Data exchanges with external entities are more at risk because FAA cannot control the schedule and priorities of these organizations. We are continuing to review FAA's progress in resolving Year 2000 issues associated with data exchanges.

End-to-End Testing Underway

Integrated, end-to-end testing of multiple systems that have individually been judged Year 2000 compliant ensures that the systems that collectively support a core business function will operate as intended. Without such testing, systems individually deemed compliant may not work as expected when linked with other systems in an operational environment. This testing should include not only those owned and managed by an organization, but also any external systems with which they interface.

In August 1998 we reported that FAA's draft end-to-end test program plan was not sufficiently detailed to provide an understanding of how the agency planned to accomplish this testing.⁸ Since that time, however, FAA has developed a detailed end-to-end testing strategy and plans.

⁸ FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998).

FAA's end-to-end testing strategy related to the NAS focuses on systems that directly support navigation, surveillance, weather, maintenance, and air traffic control functions. While most of the systems that support these functions are owned and managed by FAA, some tests include external systems with which FAA systems interface, including commercial voice and data telecommunications systems, National Weather Service systems, and international air traffic control systems.

FAA established plans for, and is in the process of conducting, three types of Year 2000 end-to-end testing: system integrity testing, operational demonstration, and field site testing. The system integrity test involves testing groups of systems that together make up a core function to ensure that data are processed correctly. FAA has identified groups of systems that support weather processing, communications, flight- and radar-data processing, and remote maintenance monitoring. The results of these tests are to be analyzed to ensure that inputs and outputs are processed correctly across interfaces.

FAA has completed two system integrity tests using systems that have passed individual systems testing, although these systems have not necessarily completed all of the steps necessary to complete validation. FAA plans to complete a third system integrity test by the end of this month.

The end-to-end operational demonstration simulates having aircraft pass through all phases of flight using recorded data and tests the activities associated with these phases—such as weather briefings, clearances, aircraft tracking, rerouting, handoffs, and transfers. This test focuses on FAA's ability to continue intersystem and inter-facility data communications through the Year

2000 date change. FAA officials stated that they completed this test last month, again using systems that had passed individual systems testing but that had not necessarily completed all validation activities.

Field site testing involves a demonstration of core NAS functions using equipment at operational air traffic control facilities in order to demonstrate that functional components at selected sites are reliable under Year 2000 conditions. FAA plans to complete this testing in April 1999.

FAA officials reported that they have encountered no Year 2000 problems thus far in any of their end-to-end tests, and plan to issue a report on the results of all three types of end-to-end testing in June. We are continuing to review FAA's end-to-end testing results.

Risks Associated with External Partners Could Affect Aviation Operations

In addition to the risks that its internal systems will malfunction or fail, FAA is at risk that external systems will fail, thereby affecting its operations. Two prime areas of concern are airports and international partners.

Many Airports May Not Complete Year 2000 Activities In Time

The successful operation of the NAS depends, in part, on the equipment that airports use to carry out their operations. This equipment helps provide safe, secure, and efficient aircraft operations and other services to the public; it includes controls for functions such as runway lighting, monitoring access to secured areas, handling baggage, providing emergency communications,

and fueling aircraft. Because much of this equipment is automated, it is at risk of Year 2000-induced failures and malfunctioning.

We recently reported on the status of airports' efforts to address the Year 2000 computing problem, based on a survey of 413 airports.⁹ While the nation's airports are making progress in preparing for the Year 2000, such progress varies among airports. Of the 334 airports responding to our survey, about one-third reported that they would complete their Year 2000 preparations by June 30, 1999. The other two-thirds either planned on a later date or failed to estimate any completion date, and half of these airports did not have contingency plans for any of fourteen core airport functions.¹⁰ Although most of those not planning to be ready by June 30 are small airports, 26 of them are among the nation's largest 50 airports.

According to FAA and airport officials, adequate safeguards are in place to ensure the safety and security of the National Airspace System through the Year 2000 date change. Specifically, FAA requires an airport to suspend or restrict operations if it is unable to provide safety and security functions. Yet, airport officials stated that they would be unlikely to suspend or restrict operations should an automated system malfunction or fail, because the airport could usually resort to manual operations. However, they also noted that if manual procedures are substituted for operations normally controlled by automated equipment, an airport's efficiency—its ability to handle its normal number of scheduled flights per day—could decrease and cause flight delays.

⁹ Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999).

¹⁰ Our questionnaire focused on fourteen core airport functions, including access control, administration, airfield operations, airport services, baggage handling, communications, environmental systems, facilities maintenance, fuel services, ground support and ramp services, navigational aids, parking, ramp operations, and weather services.

Delays at one airport could cause delays at other airports and eventually reduce the efficiency of the entire National Airspace System.

International Activity Is Continuing

American international carriers operate in over 90 countries and at over 200 foreign airports; similarly, over 125 foreign carriers cross FAA-controlled airspace. FAA lacks the authority and resources to ensure compliance of any foreign air traffic control system, but it nevertheless retains responsibility for ensuring safe, reliable aviation services for American travelers into 2000 and beyond.

FAA's Year 2000 international management team has been active. FAA is sharing information with its foreign counterparts and assisting them in addressing Year 2000 issues, such as business continuity and contingency planning. FAA is also actively working with the International Civil Aviation Organization to obtain Year 2000 status information on its international counterparts, and is prioritizing countries based on perceived risk in order to determine the level of end-to-end testing to be performed with these countries. FAA intends to complete international end-to-end testing with several countries by October 1, 1999, and plans to test interfaces with other countries after this date at their request.

FAA's Year 2000 international manager stated that FAA will provide status information on individual countries to the State Department to help develop travel advisories for at-risk countries. The State Department intends to issue such travel advisories later this year.

Comprehensive Business Continuity and Contingency Planning is Crucial

Because of the risk of anticipated and unanticipated failures—whether from internal systems or due to reliance on external partners and suppliers—a comprehensive business continuity and contingency plan is crucial to continuing core operations. FAA drafted a Year 2000 Business Continuity and Contingency Plan in December 1998, and is currently reviewing it. The agency plans to release four more iterations of this plan by the end of the year, with the next version due out in April 1999.

We reviewed the draft plan and found that it does not yet fully address several broad failure scenarios that could affect aviation operations, including simultaneous Year 2000-related failures of systems across the country, widespread power outages, or failures of interfacility telecommunications. The plan relies on FAA's current way of handling such problems at a single facility—by having adjoining facilities support the failed facility. This approach may not be appropriate should Year 2000-induced failures affect adjoining facilities. However, FAA's Year 2000 program manager stated that the agency plans to determine whether current contingency plans are sufficient to address widespread outages.

FAA is also working to address a concern with its plan that was voiced by the National Air Traffic Controllers Association (NATCA) over 8 months ago. At that time, NATCA officials stated that the contingency plans for certain FAA facilities do not adequately define the role of the air traffic controller. NATCA officials explained that should some "worst case" Year 2000 scenario occur—such as a critical facility's losing all power—FAA contingency plans require surrounding facilities to take over the air traffic control responsibilities of the failed facility.

However, the contingency plans do not specify how the surrounding facilities would assume or perform these responsibilities. For instance, it is not clear which controllers would pick up which sectors of airspace, or even what information would be available to them.

Last month, FAA's air traffic operations division requested that regional air traffic division managers work with facility managers and NATCA representatives to ensure that facility contingency plans contain sufficient detail to fully inform air traffic controllers of their respective roles and responsibilities, and to provide them with the necessary information to meet those responsibilities. This effort is to be completed by April 30, 1999.

This concludes my statement, and I would be happy to respond to any questions that you or other members of the Subcommittees may have at this time.

(511721)

Mr. HORN. We thank you very much for that very succinct statement. We are going through all of the witnesses first, and then we will have questions for all panelists.

I am delighted to present now the Deputy Secretary for the Department of Transportation, Mortimer L. Downey. Welcome.

Mr. DOWNEY. Thank you, Chairman Horn and Chairwoman Morella, for this opportunity to report on DOT's efforts to resolve the Y2K problem. I have a longer written statement which I would like to submit for the record.

Mr. HORN. Automatically, all statements are put in the record the minute I mention your name.

Mr. DOWNEY. I am here today fully confident that all DOT's vital computer systems will effectively make the transition on January 1, 2000. I am sure most of you realize that OMB has classified DOT as an agency that is making limited progress, and that congressional evaluations have continually ranked us at the low end of government.

While I understand how these determinations are made, they should not be taken as showing any lack of effort or commitment. Indeed, extraordinary effort is being applied to this challenge by many dedicated DOT employees, including Ms. Garvey and her staff and the IG's office, whose seal of approval goes on before any of our reports go out. We also appreciate the role of GAO, the questions that they raise as well as the model plans they have to guide our efforts.

As of last Friday, March 12th, 64 percent of the Department's 607 mission-critical systems were Y2K compliant, as compared with our February report of 53 percent. And since this rate of progress is not linear, I should note that 85 percent are projected to be compliant by March 31st.

The FAA projects completion of its work by the schedule that they had set, which is the end of June 1999, and they have met their other goals to date. At that time, the end of June, approximately 99 percent of the Department's systems will be compliant.

Those systems projected to be completed after June belong to the U.S. Coast Guard. The Coast Guard has scheduled completion of its final system, the Valdez, Alaska Vessel Traffic System, for October 1999. Due to complicated logistics and the weather conditions in Alaska, it is not possible to accelerate this project any further.

I will continue to work closely with all of our DOT Administrators to ensure the success of our remediation efforts, but even with confidence that we have that our goals will be reached, we are preparing and will continue to refine comprehensive business continuity and contingency plans for each of our administrations to ensure that vital services will continue to operate; whatever the cause might be for any system failure.

With respect to the broader challenges, we have aggressively reached out to our transportation partners, domestic and international, in all modes, land, sea and air, and will be happy to comment on those today. There has been a productive exchange of information which will continue, and we will inform this committee and the public of any potential areas of concern.

In conclusion, I would like to reiterate the commitment that Secretary Slater and I have to ensuring that all DOT systems will op-

erate properly before, during and after the millennium change, and we will keep you advised of our progress over the coming weeks and months.

[The prepared statement of Mr. Downey follows:]

STATEMENT OF THE HONORABLE MORTIMER L. DOWNEY
DEPUTY SECRETARY
U.S. DEPARTMENT OF TRANSPORTATION
BEFORE A JOINT HEARING OF THE

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND
TECHNOLOGY

AND THE

HOUSE SCIENCE COMMITTEE
TECHNOLOGY SUBCOMMITTEE

MARCH 15, 1999

Chairman Horn, Chairwoman Morella, Committee Members: thank you for this opportunity to report on the Department of Transportation's (DOT, or the Department) efforts to solve the Year 2000 (Y2K) problem. I appear before you today fully confident that all of our vital computer systems will effectively make the transition on January 1, 2000.

Secretary Slater and I remain fully committed to meeting the Y2K challenge. Each of our ten administrators have been charged with leading the effort to fix the problems in their systems, and they are *personally* accountable for their progress. In my monthly meetings with each administrator, the first topic on the agenda is Y2K progress. Secretary Slater and I have been unwavering in our expectations for this Agency: every mission-critical system at DOT will be repaired, replaced, or retired by the 2000 deadline. *Period.* We'll also ensure that back-ups or alternatives are available to handle contingencies and unexpected disruptions so that the public can be served with safety.

I'm sure most of you realize that the Office of Management and Budget (OMB) has classified DOT as an agency that is making limited progress, and that Congressional evaluations have continually ranked us near the bottom in government. While I understand how these determinations are made, they should not be taken as showing a lack of effort. Indeed, extraordinary effort is being applied to this challenge by many dedicated DOT employees. DOT got off to a slow start on this complex task, which prevented us from meeting all of the OMB target dates. In addition, we have consistently reported that completion of the testing process for all components of the national airspace system, including comprehensive end-to-end testing, would not be possible within the target dates established by OMB.

As of March 12, 1999, 64% of the Department's 607 mission-critical systems were Y2K compliant, and since this schedule is not linear, I can report that 85% are projected to be compliant by March 31, 1999. I reconfirmed this projection last week and have been assured that it is valid. The Federal Aviation Administration (FAA) is projecting completion of its work by the end of June 1999, at which time approximately 99% of the Department's systems will be compliant. The FAA has consistently met its projections to date, and I expect them to continue to do so. Our Inspector General will continue to work with the agencies to verify their reports.

The systems projected to be completed after June belong to the U.S. Coast Guard. The Coast Guard has scheduled completion of its final system, the Valdez Vessel Traffic System, in October 1999. Due to complicated logistics and weather conditions in Alaska, it is not possible to accelerate the project any further. The Commandant has assured me that the Coast Guard will accomplish its mission, as it has on so many other occasions. I will continue to work closely with all the Administrators to ensure the success of our Y2K remediation efforts.

Even with the confidence we have that our goals will be reached, we recognize that we must prepare for the worst: system failures that could disrupt vital services. The Department is preparing comprehensive Business Continuity and Contingency Plans to ensure that vital services will continue to operate. FAA's comprehensive plan will cover not only the national airspace system, but everything that FAA does. As Administrator Garvey will explain, the planning process has drawn upon input from many industry groups, and the final version is now undergoing a thorough internal review prior to formal publication.

The Coast Guard is also preparing a comprehensive service-wide plan which is scheduled for testing in July, as are the other operating administrations and the Office of the Secretary. In addition, we are working closely with the President's Council on Y2K Conversion and the Federal Emergency Management Agency (FEMA) to establish a coordinated crisis management capability for the days immediately preceding and following key date changes.

With respect to the broader challenges, I am serving as the Chair of the Transportation Sector Working Group under the auspices of the President's Council. We have aggressively reached out to our transportation partners, domestic and international. There has been a frank exchange of information on many levels, and from this exchange we have been able to determine several common themes regarding sector readiness:

- there is a high awareness of the problem and its potential consequences;
- there are aggressive efforts being made to combat the problem, although better progress is reported by large companies and organizations;

- predicted disruptions are relatively localized in nature but could be exacerbated by a lack of preparedness of small and medium sized organizations, or mitigated by appropriate public and private steps; and,
- there is a larger potential for international failures, adversely affecting our domestic and cross-border operations.

We will continue to work with our sector partners in each transport mode and to refine our information. We will inform the public of any potential areas of concern, both domestic and international.

In conclusion, I would like to reiterate the commitment that Secretary Slater and I have to ensuring that all DOT systems will operate properly before, during, and after the millennium change. We will keep you advised of our progress in the coming weeks.

Further, we recognize our responsibility to the traveling public and the need for us to continue our efforts to reach out to the transportation industry and all those responsible for our transportation infrastructure.

Thank you. Now, I'd be happy to answer any questions you may have about our departmental systems or about the broader transportation challenges.

Mr. HORN. Thank you, Mr. Secretary.

We will now move to Ms. Garvey, a very distinguished Administrator in the past and currently, the Administrator of the Federal Aviation Administration.

Ms. GARVEY. Thank you very much, Chairman Horn and Chairwoman Morella. It is a pleasure to be here this morning to address the Y2K efforts of the FAA.

Let me say at the outset that we have made tremendous progress, and I appreciate the General Accounting Office's comments in particular. We have made tremendous progress since I first appeared before this committee in February 1998. Since that time we have worked virtually around the clock to ensure that our skies would be safe and that air traffic will be as efficient as possible come midnight December 31st.

Within the past year, we have caught up with much of the rest of the Federal Government, and I believe we may have surpassed the expectations of many people. I realize that you, Mr. Chairman, and many members of this committee have some concerns, and I hope that I can answer some of those concerns today.

Currently the agency is in the validation phase, during which all repaired systems must be tested to ensure that all of the work accomplished during the renovation phase is complete, is correct, and is consistent. As of February 28th, we validated almost 80 percent of our mission-critical systems. We fully expect to complete validation for 100 percent of all of our systems by March 31st. That figure is for mission-critical and non-mission-critical.

Our validation process includes an independent verification and validation review by an outside contractor, as well as some very helpful work from the IG's office. It also includes comprehensive end-to-end tests which test the interrelationships of our systems and whether the individual fixes will actually work together as a whole. In particular, we will be conducting an end-to-end test of FAA's operational facilities in Denver, CO on April 10th.

As you know, after a system has been validated, it progresses to the implementation phase for key site testing and deployment. We have scheduled implementation to be completed, as the Deputy Secretary said, by June 30, 1999. Let me also stress while we will complete implementation by June 30th, we will continue to test and retest our systems for as long as possible and as rigorously as we can to make absolutely sure that we are prepared.

Let me briefly mention our agency's contingency plan. The key to a successful contingency plan is involvement, we know, of our labor partners. Last October, the FAA briefed representatives from several unions on our contingency plan. That was followed by a series of workshops and meetings from October to December, resulting in a draft version of the contingency plan.

As GAO has testified, the first version of that plan will be released on April 15th. We will continue to review that plan and to revise it as needed. We are working very closely with our labor unions on that issue. It is important, we think, to have a good contingency plan facility-by-facility. We see the development of the contingency plan as an evolutionary process.

Within the aviation industry, we have sponsored several "Industry Days," which bring together key stakeholders from all sectors

of the aviation industry. In addition, at the request of the President's Council on Y2K Conversion, we established an aviation industry Y2K steering group and a FAA outreach team. The purpose of this effort is to identify the issues, to develop a coordinated approach to solutions and, finally, to avoid duplication of effort.

The steering committee is chaired by the FAA and membership includes leaders from a number of industry trade organizations. The committee meets biweekly and is responsible for keeping industry and government executives informed of the status of the Y2K effort.

Airport readiness is another area of our outreach. I know this is a concern to members of the committee, given the GAO's recent report on airport readiness. GAO has appropriately raised some concerns in this area. I want you to know that the FAA is doing everything within our regulatory powers and even beyond to help airports achieve Y2K compliance.

We are focused first and foremost on those elements that have the greatest effect on airport safety and security. We have provided a list of commonly used airfield equipment that use computers or embedded microchips. We have set criteria for verifying Y2K readiness of airport equipment, and we have detailed a 10-person FAA team to monitor progress by airport operators. The FAA wants to ensure, in fact we must ensure, that the airports achieve compliance with our safety regulations even if they cannot be fully Y2K compliant.

Internationally, our work encompasses several efforts. Last April, the FAA issued a Y2K International Project Plan, outlining an effective strategy of cooperation and coordination with our international partners. We are working very closely with the International Civil Aviation Organization [ICAO], and the International Air Transport Association. An FAA employee has been assigned to work full-time with ICAO in their Montreal, Canada office to offer guidance and support for their Y2K coordination efforts. Both the Deputy Secretary and I had an opportunity on individual occasions to be briefed in Montreal over the last 2 weeks.

Last September, I represented the FAA at the ICAO general assembly in Montreal, where the United States sponsored two resolutions. Both resolutions, I am pleased to say, were accepted. One directs the ICAO Secretary General to develop and publish standard Y2K assessment criteria. That was completed and issued at the end of January. The second resolution urges States to submit to ICAO the status of their Y2K readiness. That information must be reported to ICAO by June 30, 1999.

FAA has also initiated informal working groups with different international entities to solve common Y2K problems. We know that cooperation between Canada, Mexico and the United States is critical to ensure that the North American air transportation system does not suffer malfunctions on January 1st. Our three countries have agreed to share information on national efforts regarding air navigation systems.

Let me say in conclusion, Mr. Chairman, while I am very proud of the progress that we have made to date, we are not overconfident. We continue to work diligently on our own Y2K challenges

while supporting the efforts of the aviation industry as best as possible.

We have overcome many obstacles to get where we are today, but we know that many challenges lie ahead. I continue to remind the Y2K team that we have got to stay the course, that each benchmark, each inch mark, if you will, is critical. Each milestone is critical.

That concludes my statement, Mr. Chairman, and I would be happy to answer any questions with my colleagues. Thank you very much.

[The prepared statement of Ms. Garvey follows:]

STATEMENT OF THE HONORABLE JANE F. GARVEY, FEDERAL AVIATION ADMINISTRATOR, BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT, SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY AND THE HOUSE COMMITTEE ON SCIENCE, SUBCOMMITTEE ON TECHNOLOGY, MARCH 15, 1999.

Chairman Horn, Chairwoman Morella, and Members of the Subcommittees:

I appreciate the opportunity to appear before you this morning to discuss the status of Federal Aviation Administration (FAA) efforts to address Year 2000 (Y2K) readiness of our systems. Ensuring Y2K readiness is one of our top priorities at the FAA, and I want to reaffirm to you and the Members of these Subcommittees that the advent of the new millennium will not bring any compromise in aviation safety with it.

I would first like to tell you about the status of the agency's efforts in ensuring Y2K readiness with our systems, and then discuss the steps the FAA has taken in reaching out to our industry and international partners. In assessing the FAA's progress towards Y2K compliance, I recall something that I told these Committees last February: that the Y2K problem is really a management problem. I also told you at that time that the FAA was about seven months behind and that I found that state of affairs unacceptable. I'm proud to tell you today that we've made tremendous progress on our Y2K problem. Although we started late, we have worked virtually around the clock since February 1998 to make sure that our skies would be safe and that air travel would be as efficient as possible come midnight December 31, 1999. Within the past year, we have not only caught up with much of the rest of the Federal government, we have surpassed the expectations of many.

I realize, Chairman Horn, that you still have concerns about the FAA's progress, but I can promise you that we will be ready as we can possibly be at the turn of the millenium, and I think that our track record over the past year can bear out that promise.

In this past year, the FAA has revamped its management approach to addressing the Y2K problem. We have not only made up for an admittedly late start, we are well on track to Y2K compliance. We built our project plan and published it in March 1998. Our plan laid out a schedule for the FAA to complete renovation by September 30, 1998, validation by March 31, 1999, implementation by June 30, 1999. We built our plan based on our knowledge of the sheer numbers of systems within the National Airspace System (NAS), and the intricacies and complexities of those systems. Our program management has been strengthened by teaming with an outside business partner, PricewaterhouseCoopers, which has the expertise to support the management and oversight of our Y2K project. Because of this approach, the FAA has been able to make significant progress towards its Y2K readiness. I am pleased and proud to say that we are on target with our plan, and we are confident that we will make a smooth transition into the new millenium.

Currently, the agency is in the validation phase, during which all repaired systems must be tested to ensure that all Y2K changes accomplished during the renovation phase are complete, correct and consistent. By February 28, 1999, we had completed validation of almost 80% of our mission-critical systems. That's 116 of 151 systems. We fully expect

to complete validation for 100% of all of our systems by March 31, 1999, mission-critical and non-mission-critical.

In accordance with the GAO's guidelines, outlined in their document "Year 2000 Computing Crises: An Assessment Guide," our validation process includes an independent verification and validation review by an outside contractor, SAIC, who, in effect, triple-checks our work. Validation also includes comprehensive NAS end-to-end tests, which test the interrelationships of systems and whether individual fixes of components will work together as a whole. These end-to-end tests are ongoing at our Technical Center in Atlantic City, New Jersey, which can simulate any of the FAA's Air Traffic Control Centers.

We will also be conducting an end-to-end test at FAA's operational facilities in Denver on April 10, 1999. Essentially, this will be a test of interfaces with the Department of Defense, and will use an FAA flight check aircraft to fly from Colorado Springs to Grand Junction to Denver International Airport. During this flight, the FAA's air traffic control computer systems will be set forward to April 10, 2000, and all of the tracking data will be recorded and sent to both the operational and the test sides of the systems. We will then review the air traffic control commands issued on the operational side of the system, and ensure that they function properly with the data that was recorded on the test side of the system. The purpose of this test is to ensure that individual system fixes will be able to work together in an operational environment.

As you know, after a system has been validated, it progresses to the implementation phase for key site testing and deployment. The implementation phase consists of rolling out Y2K changes to hundreds of FAA facilities across the country and ensuring that the systems perform adequately in their real-time environment. Our implementation phase is scheduled to be complete by June 30, 1999. All FAA systems will be fully compliant by that time, a date that we have accelerated from our original estimate of November 1999. We are continually evaluating our schedule and accelerating it wherever possible to meet OMB's implementation deadline of March 31, 1999, for mission critical systems. Moreover, although we will be done with implementation by June 30, we will continue to test, and re-test our systems for as long as possible and as rigorously as we can, just to make absolutely sure that we are as prepared as we can be for the turn of the millenium.

In addressing our Y2K problems, we have not only "patched" problems, we have developed long-range management strategies for a more far-sighted transition into the new millenium. For example, in one particularly important arena, FAA has developed a well-defined strategy for the successful transition of the HOST computer, one of the core air traffic control systems, into the next century. We have scheduled to replace the existing system entirely by 2000. However, as a contingency to HOST replacement, FAA completed renovations activities of the existing HOST by July 31, 1998, two months ahead of OMB's September 30, 1998, renovation deadline. If there is a need for the existing HOST to be operational in the Year 2000, we are confident that it will transition to the new millennium in a routine manner.

At this point, I would like to tell you about some of our outreach and collaborative efforts with industry and international partners. Although our regulatory authority does not address all the unique problems that the Y2K technology problem may create for the aviation industry, wherever the FAA has been able to, we have been as aggressive as possible in our outreach efforts to help our industry and international partners achieve Y2K compliance.

First, as the FAA developed our Y2K Business Continuity and Contingency Plan (BCCP) the agency-wide contingency plan, we realized that the plan would require significant input from our labor partners. Last October, the FAA briefed representatives from several unions on the BCCP, and requested that they participate in further development of contingency planning. The FAA followed up by planning and facilitating workshops with the labor unions from October through December 1998. On December 31, 1998, the FAA released the draft version of the BCCP. The agency is currently reviewing the BCCP internally and the first version, Version 1.0, will be released on April 15, 1999, with updated versions scheduled for July 15, October 15, and December 15, 1999. The BCCP continues to expand and evolve, as we complete our Y2K fixes, and we will review and revise the BCCP as required.

Another significant piece in solving the Y2K puzzle is coordination with members of the aviation industry, both domestically and internationally. Domestically, FAA has sponsored several "Industry Days," which bring together key stakeholders from all

sectors of the aviation industry to raise awareness and work together to solve Y2K issues specific to aviation safety and efficiency. Industry Day events typically include participants from the FAA, as well as representatives from airlines, airport authorities, aircraft manufacturers, utilities, the communications field, and international groups. Over 140 participants from all sectors of the aviation community attended the most recent Industry Day, held in October 1998, as we focused on identifying Y2K issues with industry partners, and working collaboratively towards potential solutions to those issues. Our next steps in outreach activities include more focused work, such as FAA-Industry Operational Y2K Contingency Planning Workshops, scheduled for March 30-31, 1999.

I am also particularly proud to note that the President's Council on Y2K Conversion recently asked the FAA to take the lead in establishing and leading a Year 2000 Government-Industry Outreach Steering Committee, and developing a comprehensive outreach program that works collaboratively with other DOT outreach efforts. The purpose of this program is two-fold: 1) to act on behalf of the FAA and aviation industry in facilitating a seamless government-industry millennium transition while ensuring continued safe operations and minimizing disruptions to efficiency; and 2) to serve as a focal point for developing a standardized and coordinated industry outreach program for the FAA. Consequently, the FAA established an Aviation Industry Year 2000 Steering Committee and an FAA Outreach Team. The Steering Committee is chaired by the FAA and is comprised of leaders from a number of aviation trade organizations. The Steering Committee is defining, developing, and implementing a standardized approach to government-industry outreach. The Steering Committee membership includes the FAA,

Air Transport Association (ATA), American Association of Airport Executives (AAAE), Regional Airline Association (RAA), Airports Council International – North American (ACI-NA), General Aviation Manufacturers Association (GAMA), and Aerospace Industries Association of America (AIA). Membership will be expanded on an as-required basis. This committee meets bi-weekly and is responsible for keeping government and industry executives informed of the status of FAA and industry Y2K readiness.

The Steering Committee's major activities include reporting on the FAA's and industry's Y2K readiness in preparing for the Year 2000 date change. Another major activity is coordination of data collection across airport operations, airline operations and air traffic services to meet the International Civil Aviation Organization's (ICAO) July 1, 1999 deadline requiring all participating countries to report on their Y2K readiness, a requirement that I will discuss further in a moment. A third major activity currently underway is identifying and resolving with industry partners major issues that impact the safety, security, and efficiency of the aviation and commercial space transportation sectors. One of those issues centers on the need to coordinate the FAA's BCCP with its industry partners. On March 30 and 31, 1999, ATA, FAA and the other trade associations are co-sponsoring a two day working session that will address airport, airline and FAA Air Traffic Control contingency planning, the workshop that I referred to earlier.

Finally, the international arena has been an important focus of FAA's Y2K efforts. In April of last year, we issued a Year 2000 International Project Plan, outlining an effective strategy of cooperation and coordination with international partners. Just this month, we issued a new plan focusing on continued international awareness, readiness assessment, and international contingency planning. FAA is working closely with ICAO to raise awareness of Y2K issues in the international community. An FAA employee has been assigned to work full-time with ICAO in their Montreal, Canada office, to offer guidance and support for their Y2K coordination efforts. Last September, I represented the FAA at the ICAO General Assembly in Montreal. There the United States sponsored a formal resolution that urges all contracting states to provide other states and airspace users with information regarding the Y2K compliance status of their aeronautical, air navigation, and airport services by July 1, 1999. The United States also cosponsored another resolution that directs the ICAO Secretary General to develop and publish standard Year 2000 assessment criteria on a timely basis and to maintain a database of Year 2000 compliance information, in order to assist states in reporting the Year 2000 compliance status of systems potentially affecting the safety of international civil aviation. Both resolutions were accepted. ICAO issued their assessment criteria at the end of January 1999, and as I mentioned before, this international body is requiring that its member countries report on their Y2K readiness by July 1, 1999.

FAA also initiated informal working groups with different international entities to solve common Y2K problems. For example, the North American Aviation Trilateral Fifth Meeting (NAAT/5) was held in Mexico City on June 17-18, 1998. From that meeting,

we realized that cooperation between Canada, Mexico, and the United States is necessary in order to ensure that the North American air transportation system does not suffer malfunctions on January 1, 2000, and beyond. The objective of NAAT/5 was to endorse cooperative efforts to commit to share information on national efforts regarding air navigation systems. This objective was finalized and agreed upon at the subsequent trilateral meeting held in Mexico City on December 1-2, 1998.

Although the FAA has made notable progress in solving our Y2K problems, the agency recognizes that Y2K presents a set of problems that has never been encountered, and that there are differing views as to how those problems should be defined and solved. FAA also recognizes that different stakeholders will have widely ranging resources and expertise in solving Y2K problems. We continue to work on our own Y2K challenge while supporting the Y2K efforts of the aviation industry as best as possible. We are committed to doing whatever it takes within our authority to assist the members of the aviation industry achieve a smooth transition to the new millennium and ensure the continued safety of our skies.

FAA has overcome many obstacles to get where it is today, and many other challenges lie in the months ahead. We have worked long and hard over the past year to get here, and I am proud of what we have accomplished and confident that we have done our job well. In fact, I am so confident of the success of our efforts, that at midnight December 31, 1999, I will be on a plane, on a commercial flight, flying from coast-to-coast, as we transition into January 1, 2000.

Thank you, Chairman Horn and Chairwoman Morella. I appreciate the opportunity to address the Committees this morning, and I would be pleased to answer any questions you may have.

Mr. HORN. Thank you. That is a very succinct statement also.

We are now honored to have with us the Inspector General of the Department of Transportation, Kenneth Mead. Are we still in the 20th year of Inspectors General, or did that finish with 1998? This is a vital resource in our government. Proceed.

Mr. MEAD. Thank you, Mr. Chairman, Madam Chairwoman.

First, a little over a year ago we testified before the same subcommittees. Our report then was not at all encouraging. We testified that FAA was then 7 months behind schedule in assessing the scope of their Y2K problems, let alone repairing the problems. There were serious questions whether the HOST computer used to control high altitude air traffic, would even make it to the year 2000, and FAA's schedule for fixing its computers was literally the 11th hour, or November of this year, leaving no cushion.

We made a series of recommendations at that hearing. Chief among them was establishing strong central management and moving up completion milestones to June 1999. FAA responded, Mr. Chairman, and responded well to all these recommendations.

Looking back, that February seems to me to mark a turning point. Commitment, leadership by the Secretary, the Deputy Secretary, the FAA Administrator, Mr. Koskinen and others, including oversight of this committee and GAO, have resulted unambiguously in a great deal of progress.

Overall, we have a much higher level of confidence today than we did a year ago that DOT mission-critical systems, such as air traffic control will indeed be Y2K compliant, and that there will be sufficient room in the schedule to address computer interface problems that may develop. However, the job is not nearly done. We can't let up; there is still much to do. Here is where matters stand.

DOT has 607 mission-critical systems. About 300 were OK to begin with; 309 had Y2K problems that had to be fixed. All but five of these have been, fixed, but this does not mean the fix has been installed at all field facilities which have a particular system.

DOT, as has been noted, will not meet OMB's March 31 milestone to have all systems compliant, and compliant means not only fixed but tested and installed in all locations. DOT expects to be 85 percent compliant by March 31st, 99 percent by June, and finished by late October.

FAA and the Coast Guard have 90 of the 91 systems that won't be compliant by March 31st. I would like to move to the display chart that each of you have to explain more fully what this means.

First, our numbers are as of February 28th. We had to have a cutoff to validate, but this is a moving target. Things have changed even since then. The 85 percent compliant figure on March 31st that you will hear about applies to the total universe of the 607 DOT mission-critical systems, which include systems not needing fixes. But let's focus for a moment on the 309 systems for which repairs were required.

First, all of the 151 FAA systems—I don't know if your eyes are good enough to read that, Mr. Chairman, mine aren't—but for FAA, all of the 151 systems which had to be fixed are fixed. Most have been tested.

The same is true for over 90 percent of the Coast Guard's systems that had to be fixed. The Coast Guard has the five systems

that as of February 28th needed to be fixed, and only two of its 66 systems which require repairs have been fixed, tested and installed at all field locations. The Coast Guard bears watching, but we are certain that they are up to the task.

Third, the 16 FAA tested systems reflects at least one of each mission-critical system has been repaired and tested. Once tested, FAA installs the fix at all air traffic facilities in the field. There are multiple units of the same computer system throughout the United States.

In other words, the same repair or fix that was made to the computer system in the laboratory must now be made at air traffic facilities throughout the United States. That is the real challenge, Mr. Chairman, for both FAA and the Coast Guard, to install the fix in the field and make sure it works.

To illustrate, as shown in red on that chart, for the 65 air traffic systems that needed to be repaired, one-third have been fixed, tested, and installed throughout the country. That means the fixes for the remaining 44 air traffic systems have to be installed at field locations between now and the end of June. That equates to several thousand locations.

For the Coast Guard, 64 of 66 system fixes must now be deployed to afloat or shore activities by the end of June. Also, we are paying special attention to the validation numbers, which is testing the fix. We found a need for FAA to be a bit more disciplined in providing support for the test results, and I think Mr. Willemssen has already alluded to that.

I point these out not to detract, Mr. Chairman, in any way from the progress that has been made, but rather to illustrate the scope and importance of the remaining work.

Second, with the short time remaining, DOT has to finalize workable contingency plans. We are concerned that FAA's two major unions, the controllers and maintenance technicians, still need to play an active role in the composition of these plans. These are the people who have to continue operations if unexpected failures occur.

Third, moving to the industry, DOT, Coast Guard, Transit, and FAA, have done a good job of injecting a high level of Y2K awareness. Can more be done? Absolutely. Our sense of industry readiness in the aviation area is that major passenger and cargo carriers are managing Y2K preparation quite well.

But we think, and I am speaking here only for the Office of Inspector General, that they should certify for the Department by November 1, large and small alike, that their systems are Y2K compliant. The Federal Transit Administration is requiring this of transit authority. We think that the FAA should require that as well. We have to make certifications to the Secretary, and the Secretary in turn to the Office of Management and Budget. I don't see any persuasive reason why regulated entities which carry passengers and cargo should not do likewise.

GAO has already touched on airports, and I won't.

Fourth, the international arena is one of continued concern. DOT has been working with various international organizations. Although awareness has increased greatly, there are at this hour far too many unknowns in other parts of the globe. We believe it is

time to develop a policy as to whether U.S. carriers or U.S. code-share flights will be allowed to fly to countries that are not known to be Y2K compliant.

Finally, I would like to close with the point that we in the Office of Inspector General stand ready to help in any way that we can. We found at all levels of the Department, regardless of the operating administration, an openness and support for the oversight and checking, and responsiveness to the recommendations that we have made.

Thank you.

[The prepared statement of Mr. Mead follows:]

**Before the Subcommittee on Government Management, Information, and
Technology, House Committee on Government Reform, and the Subcommittee
on Technology, House Committee on Science**

U.S. House of Representatives

For Release on Delivery
expected at
10:00 a.m. EST
Monday
March 15, 1999
Report Number: FE-1999-072

The Year 2000 Technology Challenge at the Department of Transportation

**Statement of
The Honorable Kenneth M. Mead
Inspector General
U.S. Department of Transportation**



Mead

Mr. Chairman, Madam Chairwoman, and Members of the Subcommittees:

We appreciate the opportunity to testify today on the Year-2000 computer program within the Department of Transportation (DOT) and the Federal Aviation Administration (FAA). Our testimony today will address these areas:

- Status of actions to fix DOT and FAA Year-2000 problems,
- Challenges ahead for DOT and FAA, and
- Outreach to the transportation industry and international community.

First, in February 1998, we testified on DOT's Year-2000 computer problems before these same two Subcommittees. At that time, we testified that FAA was 7 months behind the Office of Management and Budget (OMB) schedule for assessing its computer systems for Year-2000 problems, and had not yet completed its assessments. There were serious questions as to whether the Host computer, which is used for control of high altitude air traffic, could make it to the Year 2000 or be made compliant, and FAA was planning to finish its Year-2000 work in November 1999.

We recommended FAA establish strong central management for its Year-2000 efforts and establish a sense of urgency, make a prompt decision on whether to repair or replace the Host computers, and move up the implementation date to June 1999. FAA has done so. Since then, a great deal of progress has been made by DOT and FAA. But, the job is not done, and there is much still to do.

DOT has 607 mission-critical systems, 309 of which had Year-2000 problems that had to be fixed. All but 5 have been fixed. As of March 12, 1999, 64 percent of DOT's mission-critical systems are compliant. DOT will not meet OMB's March 31 milestone to have all systems compliant. It expects to be 85 percent compliant by the end of March, 99 percent by June, and fully compliant by October 1999. FAA and Coast Guard account for 90 of the 91 systems that will not be ready by March 31. FAA plans to finish its work by June 1999, and Coast Guard plans to be done by October 1999.

Second, we have a much higher level of confidence today than we did a year ago that DOT's mission-critical systems, such as air traffic control, will be Year-2000 compliant before October 1999. It should be recognized that FAA has fixed at least one of each mission-critical system that required repairs, and the repaired work has been tested in a test-center environment. FAA is now making that same repair to multiple units of the same system at air traffic facilities in the field. For example, 65 of FAA's Air Traffic Control systems have computers that must be fixed at about 3,700 locations.

No matter how extensive the search, there are no guarantees that all Year-2000 glitches will be found. So, prudent management dictates that DOT prepare workable Business Contingency and Continuity Plans. In FAA's case, the plans have yet to be completed. They should be accomplished in cooperation with its labor unions whose members will keep the system operating if unexpected failures should occur.

Finally, DOT has taken an active role in reaching out to the transportation industry, which has resulted in a high level of Year-2000 awareness. As for the U.S. airline industry, FAA, the Air Transport Association, and the industry itself have made considerable efforts at Year-2000 outreach and awareness.

Our sense of industry readiness is the same as that of the Senate Special Year 2000 Committee, namely, the major passenger and cargo carriers are managing the Year-2000 preparation well. Our confidence level with regard to the entire industry, particularly small carriers and suppliers, would be stronger if a certification of Year-2000 compliance was required of them by November 1999. FAA had such a plan last year, but it was withdrawn. The reporting required by OMB and the Secretary, in effect, requires such a report with respect to systems under Federal control, but not from the industry itself.

Regarding airports, GAO's work strongly indicates that Year-2000 compliance efforts in this area need to be stepped up substantially. GAO noted that many airports are not following a comprehensive and structured approach for repairing systems and, consequently, are at risk of experiencing some equipment malfunctions.

While DOT is getting close to fixing its internal systems and becoming more informed of the private sector's Year-2000 readiness, the same level of comfort does not exist with international transportation readiness, such as foreign air traffic control. DOT has been working with international organizations, such as the International Civil Aviation Organization and the International Maritime Organization. Both organizations have had "industry days" to increase awareness of the Year-2000 problem. However, DOT has not received status report of their members' Year-2000 readiness. Because of this, there are lots of "unknowns."

Answers are needed for the "unknowns." In our opinion, policy should be developed as to whether U.S. carriers or U.S. code share flights, cargo or passengers, will be allowed to fly to countries that are not known to be Year 2000 compliant.

Current Status

OMB established a five-phase approach for addressing Year-2000 computer problems. Milestones established by OMB are:

Year-2000 Phases and Milestones

YEAR-2000 PHASES	TASKS	OMB TARGETS
Awareness/Assessment	Determine Scope of Year-2000 Problems	June 1997
Renovation	Fix Year-2000 Problems	September 1998
Validation	Test the Fix	January 1999
Implementation*	Install Year-2000 Compliant Systems	March 1999

*A system is not counted as "implemented" until the fix is installed at all field locations and tested.

DOT has 607 mission-critical systems, of which 309 needed to be fixed (renovated) in order to be Year-2000 compliant. As of February 28, 1999, the status of the 309 systems that needed to be fixed was:

	Systems	Renovated	Validated	Implemented
DOT	309	304 (98%)	248 (80%)	101 (33%)
FAA	151	151 (100%)	116 (77%)	41 (27%)
USCG	66	61 (92%)	52 (79%)	2 (3%)

FAA expects to complete all of its Year-2000 work by June 30, 1999. The following chart shows FAA still has lots to do, in a short time, to implement the fixes for its 151 mission-critical systems.

	Systems	Implemented 2/28/99 (Actual)	Implemented 3/31/99 (Projected)	Implemented 6/30/99 (Projected)
FAA	151	41 (27%)	97 (64%)	151 (100%)
ATC	65	21 (32%)	34 (52%)	65 (100%)

One of the systems that received a lot of attention at the last hearing, and has since been repaired, is the existing Host computer. FAA initiated procurement of new Host computers, but it also took action to repair the existing computers. FAA contractors did not identify any Year-2000 problems with the Host microcode (machine language) that would preclude transition into the next millenium. FAA plans to complete replacement of the existing Host computers by October 1999. The replacement is on schedule. So far, replacement systems have been installed for use at 10 of the 26 centers.

Coast Guard has identified 66 mission-critical systems requiring Year-2000 fixes and has repaired 61 systems. One of its systems--the Vessel Traffic System on Prince William Sound--will not be repaired until October 1999. This system controls ship movements in maritime ports. The delay occurred because Coast Guard decided to replace, rather than fix, the old system.

Challenges Ahead

Testing of Repaired Systems

The Department has completed testing over 80 percent of the repaired mission-critical systems. Our office has performed independent reviews of selected systems, and alerted senior management to issues requiring further actions. For example, on February 12, 1999, we reported that there was inadequate support for test results on 5 of the 7 ATC systems we reviewed. The documentation problems we found does not necessarily mean that the fixes have not been made. It is possible that the staff at the location that did the work can demonstrate that the job was done properly. In fact, at two locations where we did an extended review, this was the situation. We are currently reviewing the remaining three systems.

FAA currently is performing "end-to-end" tests of selected ATC systems in the areas of flight monitoring, weather, communications, and remote system maintenance. These tests simulate real time air traffic operations, to include

interfacing with multiple ATC systems. While an important step in the process, end-to-end testing is not a substitute for the individual ATC system testing.

FAA plans to perform four end-to-end tests on 30 to 40 ATC systems. FAA has completed two tests, and plans to complete the rest by April 1999. These tests are performed primarily at the FAA Technical Center with test machines on-site, not the hundreds of computers and scenarios that make up the real ATC environment. Tests that have been done to date were successful with only minor glitches. FAA plans to do field site testing at the Denver En-route Center in April on systems that are operational in the field.

Interfaces with foreign air traffic control organizations are not part of these end-to-end tests. FAA knows 12 of its 20 En-route centers interface with foreign countries to handle international flights. FAA plans to test interfaces with seven international countries--Canada, Mexico, Japan, Bahamas, United Kingdom, Dominican Republic, and Cuba--which account for 60 percent of international flights. These plans are not yet finalized.

Coast Guard also has interdependent systems which, if not working together, could disturb its critical missions. Coast Guard currently is planning its End-to-End testing work.

Implementing Repaired Systems

With less than 300 days to the Year 2000, DOT still has significant challenges ahead. FAA is facing a unique implementation challenge. The ATC system fixes, after being operated in test-center environments, have to be installed at multiple sites throughout the system. For example, the Terminal Doppler Weather Radar system provides detection of weather events such as wind shear and microbursts. FAA renovated the computer used to support this system, and has to install it at 47 sites. Implementing repairs into the real operational environment has risk due to potential complications resulting from local adaptations to ATC systems (changes made by local technicians). In the past, FAA has encountered problems installing test-center solutions at locations throughout the ATC system due to local changes.

FAA has 21 of the 65 ATC systems that have been fixed, tested, and installed at field sites. The remaining 44 systems are the most complex, and have to be installed at about 3,000 field sites in the next 3 months. This very aggressive schedule has to be carried out in conjunction with the development of other major ATC modernization projects, such as the Host replacement system.

As of February 28, 1999, Coast Guard has implemented only 2 of its 66 mission-critical systems. Like FAA, Coast Guard also has to install repaired

systems at multiple sites. Some of the "sites" are vessels stationed or operating at sea. Installation of repaired systems can be done only when vessels are in port, which causes delays in implementation of compliant systems.

Completing Business Continuity and Contingency Plans (BCCP)

The development of a BCCP is needed in the event of computer failures. Of the 12 DOT Operating Administrations, 4 have completed draft BCCPs. The others are in the development process.

For FAA, a draft business continuity plan has been prepared and is currently being revised. FAA also has been trying to get more union participation, especially from its two key unions, Professional Airways Systems Specialists (PASS) and National Air Traffic Controllers Association (NATCA). In case of unexpected system failure, it is the members of these unions that must continue operations. So far, NATCA and PASS have not played as active a role as they need to in FAA's development of its contingency plan. It is essential that FAA, and its unions, develop contingency plans acceptable to, and agreeable by, all parties. DOT needs to step up its efforts to complete this important task.

Outreach to Industry and International Partners

DOT has taken an active role in increasing the transportation industry awareness of Year-2000 problems, and is making financial assistance available through DOT's grant programs. These actions are paying dividends because DOT is getting more information from the private sector on their Year-2000 readiness.

Our sense of industry readiness is the same as that of the Senate Special Year 2000 Committee, namely, the major passenger and cargo carriers are managing the Year-2000 preparation well. Our confidence level with regard to the entire industry, particularly small carriers and suppliers, would be stronger if a certification of Year-2000 compliance was required of them by November 1999. FAA had such a plan last year, but it was withdrawn. The reporting required by OMB and the Secretary, in effect, requires such a report with respect to systems under Federal control, but not from the industry itself.

The Year 2000 computer problem has important implications for the aviation industry, including airports, aircraft manufacturers, parts suppliers, air carriers, and repair stations at home and abroad. As recently reported¹ by the GAO, U.S.

¹ General Accounting Office, Year 2000 Computing Crisis: Status of Airports' Efforts to Deal with Date Change Problem, (GAO/RCED/AIMD-99-57), January 1999.

airports have made progress in preparing for the Year 2000. GAO noted that many airports are not following a comprehensive and structured approach for repairing systems and, consequently, are at risk of experiencing some equipment malfunctions.

While DOT is getting close to fixing its internal systems and becoming more informed of the private sector's Year-2000 readiness, the same level of comfort does not exist with international transportation readiness, such as foreign air traffic control. DOT has been working with international organizations, such as the International Civil Aviation Organization and the International Maritime Organization. Both organizations have had "industry days" to increase awareness of the Year-2000 problem. However, DOT has not received any status report of their members' Year-2000 readiness.

We are working closely with the Secretary and Deputy Secretary, the Federal Aviation Administrator, the Commandant of the Coast Guard, and the Department's Acting Chief Information Officer to make sure DOT's Year-2000 program goes as smoothly as possible. We will continue to monitor the issues we have discussed, and advise the Congress, the Secretary and Deputy Secretary of Transportation, the Federal Aviation Administrator, and the Commandant of the Coast Guard of progress and problems.

Mr. Chairman, Madam Chairwoman, this concludes our statement. I would be pleased to answer any questions.



Status of Year-2000 Computer Problem

Status of Mission Critical Systems Requiring Repair (as of 2/28/99)

	NUMBER OF SYSTEMS	RENOVATED	VALIDATED	IMPLEMENTED
DOT	309	304 (98%)	248 (80%)	101 (33%)
FAA	151	151 (100%)	116 (77%)	41 (27%)
USCG	66	61 (92%)	52 (79%)	2 (3%)

Schedule for Completing FAA Year-2000 Repairs

	NUMBER OF SYSTEMS	COMPLIANT AS OF 2/28/99	PROJECTED COMPLIANT 3/31/99	PROJECTED COMPLIANT 6/30/99
FAA	151	41 (27%)	97 (64%)	151 (100%)
AIR TRAFFIC CONTROL SYSTEMS	65	21 (32%)	34 (52%)	65 (100%)

Mr. HORN. Thank you very much. My co-chairman and I will be alternating and questioning for about 5 minutes each until we get through all 200 questions that we have prepared here. Don't worry, it is only 190.

Let me ask the Secretary a couple of things here.

Do you concur that those are accurate figures as far as you see? Those are generally developed by your people, and the IG has gone in to look at it and I would ask Mr. Mead, are you pretty sure those figures are sound?

Mr. MEAD. Yes, sir, as of the end of February. Mr. Downey alluded to some more recent figures that we haven't validated yet, and that is why I was not sourcing those.

Mr. HORN. February 12th was of course the quarterly report and that is what we based our judgment on. Is there anything new that wasn't in this chart of the Inspector General?

Mr. DOWNEY. We issue a monthly report to the OMB that was validated by the Inspector General. That is the report that would bring us up to 57 percent. The 64 percent was our informal review as of Friday, and before you get a monthly report at the end of this month it will also be validated by the IG, but that is the one that we expect to be at 85 percent.

Mr. HORN. Besides seeing how rapidly an agency is implementing the testing and getting full compliance, we had four other criteria which the Department of Transportation was simply, "in progress," whether it was 1 percent progress or 200 percent progress we don't know. On the contingency plan, it was in progress. What is the contingency plan of the Department of Transportation?

Mr. DOWNEY. There will be about a dozen separate contingency plans, one for each of the major administrations. By the end of this month I think most of them will be complete in draft. Some of them will be issued in final. All of them will continue to be worked on right up to the end of the year as we work with other partners, because there will be contingency plans not only for things that should be within our control but for contingencies that will be beyond our control.

Mr. HORN. Can you give me one example of one system that you have a contingency plan for?

Mr. DOWNEY. We have a full published contingency plan for the Federal Railroad Administration. It covers the internal systems of FRA. It also covers our work with the industry on safety related matters for the industry. We can provide that to you.

Mr. HORN. What is the particular system you have that is the contingency? Is it another system in another agency or what?

Mr. DOWNEY. Well, for example, in Federal Rail one of the major systems is managing our Federal inspection activities. We can fall back to do it by paper and pencil, but we want to be sure that the business functions can continue.

Mr. HORN. Have people in the Federal Railway Administration, have they been checking on microchips and what it might mean to their signaling?

Mr. DOWNEY. Yes. Throughout the industry we have worked with the railroads, large and small, and have found that signal systems, locomotives, crossing gates and all of the other safety-related equip-

ment within the industry should perform well. While there are numerous microchips, they are all event-sensitive and not date-sensitive, and so we should see those systems working.

The thing that the industry is continuing to work on, and we are monitoring their progress, is the interrelated systems they have for managing freight cars and managing the flow of traffic. Those have to work not only within each railroad but across the entire industry. The American Association of Railroads has taken the lead on that, and is working with each of the major carriers to be sure that their systems will work together. The current report we have from them is that they are about 85 percent complete with the implementation and expect to meet a June 30th deadline.

Mr. HORN. Besides completion, our second criteria on the February 12th reports was the degree to which your telecommunications system would be able to serve the computers on this. Is that true?

Mr. DOWNEY. We are including those telecommunication systems which are under our own control, such as FAA and Coast Guard systems, as part of our modernization and implementation efforts. We have to work with the telecommunication carriers where we are involved in using commercial systems. We are continuing to work with them, along with FCC and the General Services Administration, to be sure that those systems will be working.

Mr. HORN. So you have your own internal systems and switches, that if say Bell Atlantic or whatever it is goes under because of some computer glitch in their switch, you have your own way of communicating with your people?

Mr. DOWNEY. In some cases, and in some cases they are directly linked through the commercial system, and in that case we have a risk in problems with the commercial system. That is one of the reasons for having our contingency plan. Should an issue beyond our control, as a Bell Atlantic or MCI switch fail, we have to have alternate means. Typically that means having alternate routings for the data flow.

Mr. HORN. Those of us that were around when President Kennedy was assassinated recall that everybody picked up the phone to talk to their loved ones or whatever it was, and the switches just broke down. Have we looked at that situation and the disaster area since? In California it will be an earthquake or something.

Mr. DOWNEY. That is something that, working through the Y2K Council with John Koskinen, the Telecommunications Working Group is involved in that discussion. There are priority uses and priority users, and I think we will have an ability to be sure that the priority uses will be met. We cannot assure that every person in America will have a dial tone on their phone, but I think the safety-sensitive activities will be met.

Mr. HORN. Our third criteria was embedded systems. To what degree are you getting into those systems and seeing what these little microchips will do?

Mr. DOWNEY. We are working that not only through the things through our own controls but through the industry. We have worked with aviation. Aviation is an easier one to work with because FAA maintains configuration control on all aircraft and real-

ly can tell us where there are chips, and they have found the areas where changes need to be made.

We are concerned in the maritime area because there are thousands of ships out there and they are all unique, and at a later point I can tell you internationally what we are doing on that. We held a conference in London recently.

We have checked out the transit systems, and we are now surveying the auto industry, who have told us informally there are no chips in our automobiles that we should worry about; but we would like to get a more formal response from them that says no individual automobile will go out of control because of a chip.

Mr. HORN. That is good to know. I have a 1988 Mercury and I love it, and I bought it strictly because of that dashboard, and something has gone wrong already because a third of it doesn't show anything, but that is OK. Just keep after them.

Just one last question on this. External data exchange, that was our further criteria. What have you got to do on that?

Mr. DOWNEY. We are working through our external data exchange. The FAA is most critical, with interchanges with the industry and with the Weather Service. My recollection is of about 1,000 areas of interchange, there were roughly 100 that might have problems and something like half of those have now been corrected, but we are working through all of our interchanges.

Other areas that are important, maybe not safety-sensitive but important, are our flow of funds to the States for all of our grant programs. The States are very anxious to be sure that those payment flows can be made, and we will be working end-to-end tests with them as well.

Mr. HORN. I am delighted to yield 6 minutes to Mrs. Morella.

Mrs. MORELLA. I must say this is a situation where I see very honest criticism of the system, with GAO, Inspector General, with our Deputy Secretary of DOT and our Administrator of FAA, criticism and cooperation, too. I think it is probably a singular exemplary example that could be followed, particularly because as we look at FAA it started, as we have all mentioned, so very, very late.

Ms. Garvey, I would like to ask you to give us your response. Will FAA be ready by June 30th with contingency plans?

Ms. GARVEY. Yes, Congresswoman, we will be ready with a contingency plan. Our first version is going to be issued April 15th and it contains two volumes. But again, those plans are going to be revised. We expect a second one to come out this summer, and then a third one in the fall, and the whole premise is that we will continue to work it.

I think one of the issues—and I might add, by the way, that I think the involvement of the unions to date, and I absolutely hear what Mr. Mead says, that that must continue and we must involve them again and again, but I think the involvement to date has made the plan a better plan. And I expect that we will continue to work it facility-by-facility so that we are prepared. I want to publicly commend both Mr. McNally and Mr. Fanfalone for their personal involvement. It really has involved the highest levels of the union.

Mrs. MORELLA. That is another element of the partnership that I commend, and I am so pleased that you are all working together

cooperatively. I am glad to hear about the fact that you also believe that you will meet that deadline.

I want to ask a question about the fact that you plan to conduct a lot of end-to-end tests in the coming weeks. When will the FAA interface with foreign air traffic control organizations as part of an end-to-end test?

Ms. GARVEY. Congresswoman, we have begun some of that testing now, particularly with Canada. NAV Canada has been a very active partner with us in conducting those tests. We have some more tests scheduled this month, around March 23rd, and we have a trilateral scheduled in May to talk with Canada and Mexico about the very issue of testing.

We are continuing to work with a number of other international partners on testing through the spring and early summer. I can give you exactly what that schedule includes, but it includes a number of countries in Latin America as well as, of course, Mexico and Canada and European countries as well. I would be happy to follow up on that, with specific schedules.

Mrs. MORELLA. And just expanding that question just a bit more, what steps will the FAA take to ensure that U.S. air carriers or U.S. code-share flights will only fly to countries that are proven to be Y2K compliant?

And then I am going to ask if Mr. Willemssen and Mr. Mead would also comment on the questions that I have asked. Maybe Mr. Downey would like to, too.

Ms. GARVEY. The code-sharing, I may defer to the Deputy Secretary.

Just to emphasize the work that we are doing with ICAO, we expect that the information that we all have internationally on June 30th is going to be very critical. I was briefed in Montreal on Friday, and I was pleased to see the work that ICAO and IATA were able to do to date, but we have some very hard decisions post June 30th, together with the State Department, with the industry, once we I think fully understand what the situation is. We will have some difficult decisions. But I am pleased with the information that is coming in and pleased with the forthrightness that really I think all of the countries have approached this issue.

Mr. DOWNEY. If I can followup on the code-share issue, which is an economic issue, we will be looking at that same information and, together with State, make two levels of public information available. One would be travel advisories with respect to foreign countries, and this would not only be with respect to their aviation systems but generally the state of play in those countries.

With respect to U.S. carrier or code-shares where U.S. tickets are being used on a foreign airline, I believe we will look at safety as the issue, not necessarily Y2K compliance but assurance of safety, as we do today. We do not allow U.S. carriers to fly into any circumstance where we believe the air travel system is unsafe, and this would be one consideration as part of that.

Mrs. MORELLA. How do you check the safety and compliance of international carriers? Do you rely on what they tell you?

Mr. DOWNEY. We do two things. We get information from the carriers. We put a lot of reliance on our review and ICAO's review of the certifying authority in the local country. We want to be sure

that if country X certifies its carriers and airports as safe, that they actually have a good regime for doing that. We publish our evaluations of those regimes, and we take with considerable doubt any statement that comes from a country whose certification regime is less than adequate.

Mrs. MORELLA. Do you feel some countries will be closed, their airports, thinking of Indonesia, some countries of that nature, their airports will be closed?

Mr. DOWNEY. We will know better after July, when we get the information from ICAO, and before September, and we have the full opportunity to evaluate it.

Mrs. MORELLA. Mr. Willemssen and Mr. Mead, do you have any comments to the series of questions?

Mr. WILLEMSSEN. In terms of contingency plans, we think that FAA has made very good progress in this area. They have put together an initial framework. I think their strategy of going forward with additional iterations makes sense, especially as they get more detail on the exact nature of the contingencies that they want to activate. There has been very good progress in that area.

Likewise in the end-to-end testing area that you mentioned, they have got some good guidance put together and some good strategies for testing the most critical air traffic systems. We are going to continue evaluating to make sure that as much thorough testing is done as possible on those most essential air traffic systems.

Mrs. MORELLA. Mr. Mead.

Mr. MEAD. Just two comments. I would agree with Mr. Willemssen. I would underscore, though, that with respect to the business continuity plans I think we need to pay special attention, as the Administrator I am certain is, to the involvement of both the maintenance technician union and the controllers, because at the individual system level if they need to use manual procedures, you definitely want their concurrence, and I am sure that they will have it.

Second, on the code-sharing, the more we look at this, I think the public disclosure or advisories may not be sufficient and that we will need policy concerning whether U.S. airlines and the code-share airlines should be flying in certain foreign airspace. We will know a lot more by June about the readiness level of foreign countries.

Mrs. MORELLA. Thank you.

Thank you, Mr. Chairman.

Mr. HORN. Thank you. Just for the record, when you hear the word "ICAO" it is not a boxer knocking somebody out. It is the International Civil Aviation Organization, which if I remember goes back to the League of Nations and it was inherited by the United Nations. That is where most people can get together and battle things out on international policy, and it is a very worthwhile organization.

Let me ask a few questions in which I also want to involve the IG and the GAO. The FAA has established June 30th to have its computer system be ready to go. Do you think the FAA will make the June 30 deadline? Mr. Mead, will they?

Mr. MEAD. Yes, I do. I would not be surprised if there are some last minute testing issues that may extend it a bit past that day,

but that is why FAA moved this milestone up from November to June, to allow that cushion for unexpected problems.

Mr. HORN. Mr. Willemssen.

Mr. WILLEMSSEN. I think it will be extremely difficult to meet that date with the kind of thoroughness of testing that we would expect on individual systems.

Mr. HORN. Well, if they won't, why won't they make the deadline? What are the factors that affect that?

Mr. WILLEMSSEN. The major factor affecting that is so many systems to implement at so many locations. Late last week the FAA program manager estimated to us that he had about 4,500 events between now and the end of June. Each event means one system at one location. Multiply that by 4,500 in a little over 3 months, and have it all go the way that it is supposed to go—with that many systems and that many locations—will be extremely difficult to do. If FAA can pull it off, great. We hope that they can. However, I am not sure that they can with the thoroughness of testing that we will be looking for.

Mr. MEAD. I would rather, Mr. Chairman, if we see in our monitoring of validation that Mr. Downey alluded to disclosures on the cutting of corners on testing, I would rather see implementation slip by 2 or 3 weeks rather than come up with a nice rosy report and later have to back off of it.

Mr. HORN. I think everybody up here shares that view, also. Let's do it right. Are those in the regional centers or in the actual airports that these events take place?

Mr. WILLEMSSEN. A range of facilities from en route centers to terminal radar approach control facilities to automated flight service stations. We counted up the different types of facilities and came up with a number of 654 different types of facilities, some with maybe one system, some with multiple systems. That is a huge challenge for any organization to have to deal with in a little over 3 months.

Mr. HORN. Ms. Garvey.

Ms. GARVEY. First of all, let me say we do not minimize the challenge ahead of us. It is a big challenge, but I really do think that we have it laid out in such a methodical and thoughtful way that will allow us to meet that challenge.

There are 100 events per sector. There are 33 sectors. We have the best technicians in the world, who know this system and have grown up with this system. In addition, we have 250 specialists also assigned to it. So while it is an enormous challenge, we have it laid out by sector in such a way that it can be met, we think. But I would certainly agree and restate what the Inspector General said: We want to make sure that the testing is accurate and valid, and we welcome the involvement of both the GAO and the Inspector General in that effort.

Mr. HORN. Any other comments to be made on this? In other words, you all agree if it is slippage of a few weeks, don't worry about it as long as we get the job done.

Mr. DOWNEY. None of us will stop worrying until the job is done.

Mr. HORN. One of the first strategies in finding out how a system will perform through the year 2000 date change is to contact the vendor of the key components to determine if the vendor will cer-

tify that their products are Y2K compliant. FAA did not do this on the so-called ARTS-III hardware. Now, why didn't we do this?

Ms. GARVEY. Mr. Chairman, we had some very intensive testing done with Lockheed Martin, and also actually with the firm that originally put together the ARTS-III, and we have had lengthy discussions with GAO as recently as Friday. We think that the testing and validation is solid and good and we expect to get a letter today from Lockheed Martin to that effect. But we also agree if GAO has some concerns, Lockheed Martin has said that they will be happy to run the testing again so we can all have a level of comfort that we need. So we stand by the testing, and Lockheed Martin has done the validation, but we are happy to run it again if that would help.

Mr. HORN. Mr. Willemssen, how do you feel about this?

Mr. WILLEMSSEN. To the extent that the contractor in this case can provide a certification that this particular piece of hardware, manufactured more than 30 years ago, is indeed Y2K compliant, that will give the Federal Aviation Administration a greater level of assurance that issues will not come up.

In terms of the software, there does need to be some additional testing done. The report that has been done thus far by the contractor indicates that the year is represented by two digits, not four. There are some Y2K ramifications possible, and we would like to see more thorough testing of the radar tracking function in particular to make sure that this issue doesn't surface.

Again, one thing to keep in mind here, you vary the level of testing depending on the criticality of the system. This system is absolutely essential. It provides flight information and identification information to controllers, and therefore we think the bar needs to be pretty high.

Mr. HORN. Well, does it also have to be earlier? As I look at the data from our own staff, these systems support critical FAA functions, as you noted, include aircraft surveillance and weather data processing, yet 12 of these systems will be among the last of the FAA systems to be completed. Is that a problem?

Mr. WILLEMSSEN. Well, it is something that we wanted to point out in the statement in terms of making sure that FAA focuses, as I testified in August, on the most critical air traffic systems, and to make sure that the thoroughness of testing is especially focused on those particular systems. So it is noted that they are later in the process but again, as mentioned a few minutes ago, to the extent that it takes even a little longer than the current milestones to make sure that they are thoroughly tested, we would support that.

Mr. HORN. Any other comments?

Ms. GARVEY. Just to reiterate, Lockheed Martin is very comfortable with it, but we would be happy to continue those discussions and further testing if necessary.

Mr. HORN. Mrs. Morella.

Mrs. MORELLA. Thank you, Mr. Chairman.

I want to first of all pick up on the contingency plan concept. Ms. Garvey, if Mr. Willemssen's suggestions that contingency plans could be in a little difficulty with regard to meeting the deadline,

which contingency plans, for which particular sector? Can you be specific?

Ms. GARVEY. There are about six systems that are critical, including the ARTS-III, as GAO has testified. In addition, HOST, for example, is very, very important to us as well. So we would focus on those particular systems that are really critical to the working of the system, the heart and soul of the system.

For example, HOST, if HOST fails, we have a backup system that would come into place and ultimately, if we are concerned enough, we would increase the separation or slow up the traffic to some degree. So those are the kinds of contingency plans, but you can look at a system like HOST, see what the backup system is and see what the backup is to that, with the ultimate being separation or further separation of the aircraft, actual delays if we need to.

Mrs. MORELLA. Mr. Willemssen, you want to comment on that?

Mr. WILLEMSSEN. I would. Again, we have been very supportive of the focus that FAA has had on the contingency planning over the last several months. They have focused from a business function perspective—that is, to look at it from end-to-end. For example, in the surveillance of aircraft, one would focus on making sure that they are still appropriately separated and looking at the various things that could potentially go wrong, and if those events realize themselves, what kind of backup they would have in place. And I think they are moving in that direction. They have a good draft in hand that is ready to be fleshed out with some more details.

Mrs. MORELLA. I see this as really very, very important because of the “house of cards” concept. One thing is connected to another. If one topples, the whole situation could be chaotic, and I guess you would agree with that.

Mr. WILLEMSSEN. Yes.

Mrs. MORELLA. It was just the other day I talked to some members. There was a conference here in the travel industry, and actually they did a reservation check and they found—it was in February, early February they found that their reservation system came through without a hitch for reservations, you know, January 2000 and beyond. However, they are obviously concerned about whether or not they will be able to fulfill these reservation contracts with their clients.

So I guess I would ask you, in terms of the connections, what about luggage systems at airports? Are you overseeing the airports’ alternative power sources, I mean, the electric generators? What about, you know, other terminal systems? Would you like to comment on some of those specifics?

Ms. GARVEY. Let me make a brief comment about that. From our perspective, from the FAA’s perspective, we are focused on those systems that are related to safety and security. Airfield lighting, for example, is absolutely critical as are the condition of the fire trucks, and whether they are actually ready and Y2K compliant.

That is really our focus. It is those elements that are part of the part 139 certification processes that airports need to go through. However, I will say that as we have the joint discussions every other week with industry, many of those other issues are coming up, and I know that ACI and AAAE and even ATA are spending

a good deal of time with the airport operators on some of those issues. But really our critical issue is the safety and security element of it.

Mrs. MORELLA. Would the rest of you agree? Would you, Mr. Willemssen?

Mr. WILLEMSSEN. I think that is the appropriate focus. Again, since there is so much to do and limited time to do it, you have to focus on those important areas.

Mr. DOWNEY. We are comfortable the FAA should put their focus on the safety side, but we are also working with the industry because if some of these other systems fail, it could have a significant effect on the movement of commerce. We don't want to see serious delays there, but it is safety first and then the other issues. We are concerned that some of the airports have not really looked at all the things they need to look at.

Mrs. MORELLA. So there are a number of entities that need to be looked at, that are not within your purview because they don't involve safety, but they certainly could involve inconvenience at a minimum, you know, minimally, and as others should be looking at. I am wondering about the cruise industry, Secretary Downey. Is there any checking on whether or not the cruise ships are Y2K compliant?

Mr. DOWNEY. Coast Guard has been working with all of the elements of the maritime industry, and had a very successful conference in London earlier this month at which a code of good practice was agreed to by the industry. We believe it will be endorsed by the International Maritime Organization, which usually takes many years to get things agreed to. I think in this case they are going to speed up their process. This will allow the Coast Guard to have a quick checklist of any ship entering U.S. waters and determine quickly what they have done and what they have not done, and under our regime of port control, we could bar ships that are not ready for the year 2000.

Mrs. MORELLA. The Coast Guard is the one who has the responsibility to deal with those vessels.

Mr. DOWNEY. The Coast Guard has the ability to deal with that in U.S. waters. We are looking at it internationally because it is an international issue.

Mrs. MORELLA. Absolutely. Right.

Thank you, Mr. Chairman.

Mr. HORN. On that very point, some have told us, looking at it on a worldwide basis, that microchips are in the refineries, they are in the ships, they are in the unloading and everything else. To what degree is the Department of Transportation concerned that we can't get a gasoline, a petroleum and oil supply into this country?

Mr. DOWNEY. We are working with the pipeline industry and the tanker industry and the refineries to assure that there will be a continuity of supply. The question of chips is a concern. We have pretty much ruled out the problem with respect to the pipelines.

They have done complete checking. The issue with the ships is a lot more difficult than with aircraft because there is not the kind of tight configuration control. This is why we were so pleased to get the major elements of the industry together, to turn the problem

over to them with a clear checklist of what they have to do. We now will know whether tankers, for example—and InterTankO, the trade association, was part of this agreement—will now have a set of steps that each operator can go through and that we can follow up on to see if in fact they have been done.

We cannot completely rule out the problem yet, especially in ports all around the world. The cargo cranes, for example, we heard when we met with Mexico a few weeks ago that they have been checking in their ports. They found half the cranes are OK but they haven't been able to verify the other half as well. So Coast Guard will be ready, as they always are, to deal with any emergencies that are generated and to be sure that we can maintain an adequate flow of critical materials.

Mr. HORN. The Department of Defense has a cooperative relationship with Russia in terms of having our officers in their air defense commands, their officers in ours. Russia provides most of the energy supply, at least gas, coming out of Russia into Eastern Europe and part of Central Europe. This whole thing, if something goes awry, is at winter season.

To what degree is the Department of Transportation offering to help Russia if they have problems? Now, it is primarily a pipeline going there. Maybe we are not worried about pipelines, I gather, but has any exchange been done between this country and Russia?

Mr. DOWNEY. Not formally, yet, but I believe there will be discussions at the very senior levels, and certainly the Department will be ready to be part of any team that is provided to Russia.

Mr. HORN. I think that is a good idea because if that system goes out of whack, you are going to have millions of Europeans freezing. They just won't have the supply for the heat.

Let me ask Mr. Willemssen, the Federal Aviation Administration has contracted with a firm, and I don't know if there is a name for it, it is SAIC. What does that stand for, pray tell? Another acronym in Washington.

Mr. WILLEMSSEN. That is how most of us refer to it, SAIC.

Mr. HORN. Is it SI-AC or what?

Mr. WILLEMSSEN. Just SAIC.

Mr. HORN. SAIC. OK. To perform independent verification and validation activities. In your opinion, are they performing both verification and validation?

Mr. WILLEMSSEN. I think it is an excellent step that FAA took, to get such a contractor into the system on this effort. One of the areas that they may want to consider is having SAIC or another similar contractor also perform work for them in addition to double-checking, so to speak, on the documentation and paperwork behind certifications. They also may want to go a bit further and have another independent source rerun some of the tests to see if indeed the same results come out of those tests as the original tests that were done. That is especially true for those systems that are most essential to the air traffic control system. Again, it is not necessary for all systems.

Mr. HORN. What are the potential consequences of not independently validating the system test?

Mr. WILLEMSSEN. Well, one thing an independent test gives you is added insurance, especially if that independent tester has a men-

tality that "We are going to try to find problems here" as opposed to, "Well, let's try to check this box and go on to the next step." You really need mentality with the organization that is doing the independent tests, in order to have some pretty rigorous test scripts that can identify potential issues that could surface themselves, if not on January 1, 2000, on some of the other critical dates. So I think that is an important consideration for FAA to keep in mind.

Mr. HORN. Mr. Mead, in your February memorandum you noted the President's Council on the Year 2000 Conversion identified computer security as a potential concern due to the magnitude of year 2000 renovation work that is being performed. So I guess the obvious question is, how vulnerable are the Department's computer systems to security threats? And is the FAA, Federal Aviation Administration, particularly vulnerable?

Mr. MEAD. I think it is fair to say that FAA as well as other parts of the Department need to step up their efforts in the computer security area, and it is a very formidable undertaking. I know DOT is not the only agency in government facing this issue, but internally it is something FAA and Coast Guard face, particularly these operational agencies.

Mr. HORN. Is there one administration within the Department of Transportation that is particularly vulnerable? Or are they all equally vulnerable? Looks like the Railway Administration, for example, doesn't have as many problems as we might have thought they would have.

Mr. MEAD. We attempted payroll penetrability a couple years ago. The system was so old it was difficult to penetrate.

Mr. HORN. You were trying to give Inspectors General an increase in pay, or what?

Mr. MEAD. That would be acceptable, too, Mr. Chairman.

Mr. HORN. Somebody's 17-year-old high school student penetrated it, right?

Mr. MEAD. Frankly, even though FAA and the Coast Guard are both operational agencies and have to take care of people's lives as part of their daily mission, it is also true that the Federal Highway Administration dispenses, large amounts of money, and so computer security is an equal concern across the board at DOT.

Mr. DOWNEY. Mr. Chairman, if I could add a bit on that, the Y2K Council has been working very closely with the Critical Infrastructure Assurance Office which is part of the National Security Council, and we really view Y2K as a dress rehearsal for what we have to do on computer security not just in the government but across all of industry. It is an important area and we have learned a lot in the last year about what we need to do.

Mr. HORN. Mr. Mead triggered in my brain the magic words, like Groucho Marx, the Federal Highway Administration. I am told back in either 1987 or 1989 a very able programmer laid it all out for him and said we ought to be doing this just like Social Security did in 1989, and the old boy network just gave no credence to a woman programmer, which is nonsense.

And what I want to know now is, in 1987-1989 the Secretary never had a chance to talk about that issue. There was no manage-

ment system within Transportation to get that idea percolating to the top so he could talk or she could talk, as the case may be.

Do any of you in these different administrations, Rail and Coast Guard and Federal Aviation, have a problem? And I would think the FAA Administrator at that time would have nodded his head, "Yes, sounds like we'd have a problem." It didn't get there. I guess I would ask the question, have the management lines within the Department of Transportation shaped up from those days?

Mr. DOWNEY. I think one of the things that will help in that regard is the creation of the Chief Information Officer position within the Department and equivalent positions. One has just been hired at the FAA. And that crosscutting network of individuals who have shared concerns, whether it is the CFO on finance or the Chief Information Officer or other comparable activities, do get us more of the sharing of activities.

We also try to work better among the Administrators, to be sure that the line activities are also well coordinated. We have a concept now called "One DOT." When someone learns something like that, sharing it is viewed as a very important activity within the Department.

Mr. HORN. So nothing like this would happen again?

Mr. DOWNEY. I would hope not.

Mr. HORN. Well, we all hope that but the problem is, is there a mechanism to get tough questions up to the top?

Let me see. Ms. Garvey, the Department of Transportation's Chief Information Officer has issued guidance cautioning that the year 2000 windowing technique, which is only a temporary fix, could result in slower system performance. What kind of fixes are the Department and FAA using to ensure that its systems are Y2K ready?

Ms. GARVEY. I am sorry, Mr. Chairman, you mean the——

Mr. HORN. Well, as I understand it from what staff have said from looking around, Transportation's Chief Information Officer has issued guidance concerning the so-called windowing technique, which is only a temporary fix, and it could result in slower system performance. Well, if it is a fix, is that going to help the Department and the FAA in the long run to really make sure you have done the job?

Ms. GARVEY. I think from our perspective, I may have to turn to staff for this, but what we are trying to do is renovate the systems that we have in place.

Are you familiar with that? Let me turn to Mr. Long.

Mr. HORN. Mr. Long, just identify yourself and give us the answer.

Mr. LONG. I am Raymond Long. I am the Director of the FAA's year 2000 project. The FAA is using a windowing technique on our existing legacy, older systems. On all of the new systems that are being deployed into the FAA, we are requiring that those contracts be modified to show four digit date expansion.

The only place for using windowing is in our legacy, older systems. We have not tested for system degradation as we are doing the window technique. It has not been a problem up until now because the air traffic control system does not use the date like your

microcomputers or your other systems. It is something we can include in our post-implementation activity if we felt we needed to.

Mr. HORN. Mr. Willemssen, do you have any comment on this?

Mr. WILLEMSSEN. Windowing is a commonly accepted technique, especially as time grows short and there is not enough time to expand all the date fields. The biggest issue that I would be concerned about, rather than a performance issue, is one of data exchanges because if a particular system has been windowed and is staying with two digits, and if that particular data is sent to another organization and they are expecting full expansion, and if the relationships and bridges have not been worked out, you risk having some degraded data going into another system. Windowing is a generally accepted technique but like all techniques, it has its risks.

Mr. MEAD. In our February comfort letter to the Secretary and Deputy Secretary on this matter, we indicated that tests on performance issues should be more robust.

Mr. HORN. OK. Mrs. Morella, 8 minutes, since I ran over. Equity is what we engage in.

Mrs. MORELLA. You're so precise. Thank you.

Secretary Downey, I represent Montgomery County, MD, and Montgomery County, MD, has been recognized nationally for its advanced transportation management system and other technologies that are used for transportation. I wondered what you are doing to work with a jurisdiction like that, particularly in terms of assisting other localities and jurisdictions with regard to what's been done and what can be done?

Mr. DOWNEY. Montgomery County has in fact been one of our poster children for good practice and good progress. We held a workshop in January at the Transportation Research Board, which is the get-together that has thousands of people from highway and transit management around the country. We got all of the entities together that have concerns about Y2K and we asked Gordon Ayogi, who is running the emergency center in Montgomery County to take everyone through what, in fact, they have done, and it was very helpful for us.

The Intelligent Transportation Society of America [ITSA], has been our partner in reaching out to traffic control, traffic information, and other computer-based systems around the country, and we think things are in pretty good shape in that area, but we appreciate the help from Montgomery County in sharing their experience.

Mrs. MORELLA. Excellent. Glad you are utilizing that with other jurisdictions.

I guess I would ask this question of maybe Mr. Mead, and Mr. Willemssen may want to comment, maybe Ms. Garvey. Actually, most completed and planned tests of the air traffic control systems have been done at the FAA's tech center. In the past, has the FAA experienced problems installing tech center solutions out in the field? Ms. Garvey, you may want to comment on it also.

Mr. MEAD. In some instances, and you'll note in our statement that we make a point, as a cautionary note, that testing in the laboratory can sometimes be different when you go into the real world. One reason for that, particularly for the FAA, is throughout the

National Airspaces system, the FAA has made local adaptations to their software systems, and for that reason, occasionally when you install something that works in the laboratory, it may not work in the field because of local adaptation. This particular factor is one that contributes to the great challenge remaining in the next 3 months.

Mrs. MORELLA. Mr. Willemssen, you want to comment.

Mr. WILLEMSSEN. I would concur with the Inspector General's comments. That is not to say that the technical center testing has necessarily been deficient, but it is to be expected that once you go with live operational testing, that you will come up with some issues that weren't fully identified or considered in the laboratory.

Ms. GARVEY. I think that is absolutely correct, and that is why the Denver test, which really is a live site, is going to be so important. And again, we very carefully laid it out step-by-step. It is going to be very carefully monitored. Obviously it is 2 a.m., so traffic will be less, but we expect that that will be very useful, very similar to what Wall Street did a couple of weeks ago in testing some of their systems. We think this is going to be a critical and important test, and we are looking forward to it.

Mrs. MORELLA. Did you say April was when you were going out to Colorado?

Ms. GARVEY. April 10th, yes.

Mrs. MORELLA. I think we all agree that this is an area that is fraught with challenges and problems. Let me ask you, first of all, would you be doing any other testing after Denver?

Ms. GARVEY. That is the one that is scheduled right now. I think a lot will depend on what we learn from that test. We don't have any other similar tests like that. We have lots of tests planned at the tech center but for live tests, that is it for right now.

Mrs. MORELLA. You may want to do that.

Ms. GARVEY. Oh, yes. And of course at each center as it is implemented will be tests, as the Deputy Secretary reminds me.

Mrs. MORELLA. I also note that a report I think is going to be forthcoming, I want to ask you about it, of what are the six most populous sites in terms of an assessment or appraisal of them, like Canada, Bahamas. Would you comment on that?

Ms. GARVEY. There are six countries where about 60 percent of the Americans travel. We are working very, very closely with each one of those. Knowing that that is such a high percentage, we are working very closely with those.

In fact, either the Secretary, the Deputy Secretary or I have met with them at some point during the last year, and in each case we will be developing a very coordinated work plan for dealing with some of the issues, the travel issues that we have. Not surprisingly, we are probably a little further along with Mexico and Canada. We have a trilateral meeting, as I mentioned, in May, and that will be discussed there.

But Joe Morgan, who leads our international effort, has worked very closely with these countries, went to Mexico and spent a good deal of time working on a plan together with them. As I mentioned earlier, we are doing the testing this month with Canada. We will follow it up with Mexico, and the other countries as well.

But that was the first critical issue that we looked at. We said, where is it? As everyone has suggested, the international presents some real challenges, so the first thing we said, are there areas where we really need to focus some efforts? Looking at those six countries where so many people travel seemed to be very important.

Mrs. MORELLA. It is interesting that 60 percent travel there.

Mr. DOWNEY. We also had, under the auspices of the Y2K Council, a meeting a few weeks ago with Canada and Mexico on all of the systems, power, travel systems, railroads, police, anything in which there is exchange across the border, and I think we have a very good working relationship with those two countries.

Mrs. MORELLA. What have you learned so far?

Mr. DOWNEY. We have learned some interesting things. Mexico, for example, has done I think a much more careful measure of how they are assessing their progress. They have a weighted average that really gives credit to how much work has been done leading up to the completion of a system so that they really know at any given time, I think better than we do, where they are on the whole process.

And of course there are—you know, there are always surprises that pop up. There is useful information exchanged about what are you hearing, what are the rumors in your country, and it turns out to be similar to the rumors in our country, but these kinds of discussions country-to-country and industry-to-industry are very helpful.

We had one the other day for all industries that lead to getting coal to the power plants. The power plants are clearly critical but they won't work if coal doesn't get there. So we had the mining industry, the barge and the railroad industry all in one room at one time. The biggest issue for the mines was elevators. They are now comfortable their elevators are going to work, for the same reason that elevators will be working in buildings.

Mrs. MORELLA. Any kind of dangerous issues that came up so far?

Mr. DOWNEY. None yet. Nothing that sort of a light bulb went off and where we said we better take critical action.

Mrs. MORELLA. Very good.

I yield back, Mr. Chairman.

Mr. HORN. Thank you. Let me just ask Mr. Downey, I have forgotten what year you joined the Department of Transportation as Deputy Secretary.

Mr. DOWNEY. Most recently as Deputy Secretary in 1993, although I was in the Department in the 1970's.

Mr. HORN. Well, you'll remember that in 1993–1994 you had that operation—I forgot, was it in Germantown or somewhere out there—were working on a new radar system. Maybe you don't want to remember it.

Mr. DOWNEY. I try to forget that.

Mr. HORN. It started before you, so you don't have to worry about it.

Mr. DOWNEY. We shut that one down, but it was a good example of bad management.

Mr. HORN. I knew that as I walked into the room. The \$4 billion was dumped. IRS did the same thing. Now, all I am asking about is not to rehash that dog but to—is that HOST a successor to that, or are you underway on some other type of successor?

Mr. DOWNEY. HOST is a piece of that and it is an interesting piece. Once we made the decision that a single contract with a single contractor for unlimited funds and unlimited time was not the way to proceed, working with the FAA, and largely these were FAA decisions, we broke the system down into a number of pieces: the display system radar at the major en route centers, which is now moving well; the system at the terminals, which is in reasonable shape although it has some problems; and then the HOST, which is the heart of the computer capacity at the centers.

At the time, 1992–1993, it was thought that the HOST could be put at the far end of this process as we did each piece, but when we came to look at Y2K issues, and similar to the question you raised earlier, the manufacturer was unable to certify this equipment. We said, whoa, it is time to accelerate that as part of the modernization process, but also as a backstop for Y2K. Having it as a separate module as opposed to part of this overall process allowed us to break out a separate contract, move that ahead.

It is going very well. In fact—was it Friday—Thursday the Administrator and the Secretary were up in New York to dedicate the first HOST, and several of them are now in business and operating regularly as part of the air traffic control system. All of them should be in place by the end of the year. If they are not, there are backup strategies to be sure they will be Y2K compliant. But breaking that massive project into a series of manageable pieces was the right thing to do, and it is working for us here as it is in the modernization effort.

Mr. HORN. So HOST is 2000 compliant?

Mr. DOWNEY. HOST will be 2000 compliant. How many centers is it now functioning? In 10 centers it is working today in a Y2K compliant mode.

Mr. HORN. And it would have to work in how many centers between now and January?

Mr. DOWNEY. Ten more have to be installed.

Mr. HORN. So it is a total of 20?

Mr. DOWNEY. Total of 20.

Mr. HORN. What is this project costing, just for curiosity?

Ms. GARVEY. In total, I would have to get the number for you, Mr. Chairman, but it is certainly far less than the number you talked about earlier.

Mr. HORN. Less than \$4 billion. But you were right to pull the plug. This was long before Ms. Garvey came to bring order out of chaos.

Mr. MEAD. \$172 million.

Mr. HORN. How much?

Mr. MEAD. \$172 million.

Mr. HORN. \$172 million is the HOST 10. How about the next 10?

Mr. MEAD. \$172 million for the whole job.

Mr. HORN. For the whole job?

Mr. MEAD. Yes. I think it is important to note that last time we testified before this subcommittee, we had run out of spare parts,

but if FAA cannot replace all 20 HOST computers in this year, they'll have enough cannibalized HOSTs to generate spare parts.

Mr. HORN. They'll no longer have to use Post-Its on the windows of the control tower?

Mr. MEAD. No.

Mr. HORN. That is reassuring to me, because I am carrying my own Post-Its in case they needed it in L.A.

Do you have any thoughts in the end, unless you have more questions?

Mrs. MORELLA. I will just ask another question, and then I'm going to ask them if there is anything they'd like us to know as we conclude this particular hearing and before we get the final report.

Actually, I guess GAO, to begin with FAA identified 26 air traffic systems as posing the greatest risk to the national airspace system that may not be operational through the year 2000, and these systems are going to be among the last FAA systems to be completed. And I guess the question is, why would the most at-risk systems be left for last, and why wouldn't—why aren't they scheduled for completion earlier?

Mr. WILLEMSSEN. I think among the reasons for that is often they are the most challenging systems to fully validate and implement at a number of facilities throughout the country. So I don't know that it necessarily was a conscious decision on their part. That is, we have no evidence that FAA said, "Well, these are the most critical so we will wait till the end."

On the contrary, the evidence we saw, as one might expect, was that those systems are among the most difficult to implement and therefore, everything else being equal, will take longer. But I think your point is a very good one, that FAA has to still focus on priorities, and we have to make sure that those most essential systems are dealt with not only timely but, as I have mentioned earlier, thoroughly. Also, someone must aggressively seek out to identify any and all problems that may occur, and there must be enough time left in the remainder of this year to address those problems.

Mrs. MORELLA. Mr. Mead, would you agree? Do you think that because they would take longer and be more critical, that they should be looked at earlier? I moved up on the timetable.

Mr. MEAD. In an ideal world, yes. These are probably the most complex of all the undertakings and because of the late start, that had a cascading effect throughout the schedule. So in an ideal world, I wish it had already been done. I am sure everybody does.

Mrs. MORELLA. Do you have a gnawing concern about it?

Mr. MEAD. No, I think FAA has a sensible plan. I know it is a compressed schedule, but I have confidence in FAA's year 2000 management. They set their mind to it. I think they can get it done.

Mrs. MORELLA. I think the FAA has been working very diligently, and as I have mentioned before and you mentioned in your opening statement, Ms. Garvey, working around the clock. It is such a tremendous system and so connected in so many ways.

Secretary Downey, also on another transportation issue, how about Metro? What are you doing to sort of coordinate what's hap-

pening, to make sure that the public transit systems are going to be compliant?

Mr. DOWNEY. We have worked with the public transportation systems around the country. We had a conference in Houston just a few weeks ago to compare notes and to share information. We have also asked, under Federal Transit Authority's general authority to regulate the funding that flows to these entities, to get that funding they have to be technically proficient, and we have set Y2K compliance or comparable safety levels as part of that proficiency. We have asked the boards of each public transit agency in the country to certify to us by the end of June that they are compliant or tell us what their alternate plans are.

So we look forward to hearing from Metro on that. I know that they work closely on this issue. I have talked with Dick White about it. I know they are having some trouble as we speak with their computer systems, but that shows that they are very much focused on making that system work and work safely.

Mr. MEAD. Mrs. Morella, I would like to just submit for the record, if it would be permissible, the letter from Administrator Linton of the Federal Transit Administration asking for all transit properties to certify their compliance before the year 2000 because this is a comparable recommendation we are making to FAA.

Mr. HORN. Without objection, that will be put in the record at this point.

[The information referred to follows:]



**U.S. Department of
Transportation**
Office of the Secretary
of Transportation

The Inspector General

Office of Inspector General
Washington, D.C. 20590

May 20, 1999

The Honorable Stephen Horn
Chairman, Subcommittee on Government Management,
Information, and Technology
Committee on Government Reform
House of Representatives
Washington, DC 20515

Dear Mr. *Mr. Horn* Chairman:

In our testimony before your Subcommittee on "The Year 2000 Technology Challenge" at the Department of Transportation, March 15, 1999, we made two recommendations to the Federal Aviation Administrator concerning FAA's Year 2000 (Y2K) computer program. Subsequent to the hearing, we issued a report asking the FAA Administrator to respond to our recommendations. On May 5, 1999, FAA responded (enclosure). Our recommendations and views, and FAA's response are summarized for your information.

Recommendation 1

We recommended that FAA take action to require key components of the aviation industry, such as passenger and cargo carriers, to provide certification of Year 2000 compliance no later than November 1, 1999, or such earlier date that FAA deems appropriate.

FAA Response to Recommendation 1

FAA did not agree with our recommendation. FAA said:

Requiring Y2K certification by the industry would not improve the FAA's position to take enforcement action against Y2K-related incidents. If an industry component is not Y2K compliant by January 1, 2000, the FAA's current regulatory authority is more than sufficient to take enforcement action and effectively deal with Y2K-related contingencies or emergencies. . . . FAA . . . has been surveying . . . industry components for Y2K status, and have assurances that most entities currently are, or will be, Y2K compliant before the end of 1999. Accordingly, the actions already being taken by the FAA fulfill the purpose of an industry certification.

The complete text of FAA comments is enclosed.

We do not agree that actions already being taken by FAA fulfill the purpose of an industry certification. Because of this, we will closely monitor FAA actions based on the data and information received from industry and international organizations, and report on potential problems, if any, as they are identified.

Recommendation 2

We recommended that FAA develop a policy as to whether U.S. carriers, or U.S. code share flights, cargo and passengers, will be allowed to fly to countries for which there is not a credible base for concluding their air traffic control systems are Year 2000 compliant.

FAA Response to Recommendation 2

FAA agreed with our recommendation and said:

The FAA is currently developing an interagency process by which the FAA will address international Y2K readiness of foreign air traffic service providers, airports and foreign flagged air carriers. . . . The FAA has been working with the International Civil Aviation Authority (ICAO) and other key international aviation community leaders, including the International Air Transport Association (IATA), to develop Y2K assessment criteria. . . . ICAO is requiring each of its member States to provide its Y2K compliance status by July 1, 1999. ICAO has also agreed to collect and publish this compliance status data . . . beginning July 15, 1999.

FAA has also proposed an interagency effort to evaluate all available international civil aviation Y2K readiness information, including the ICAO self reports. . . . The FAA plans to convene an evaluation panel, comprised of representatives from FAA and the Departments of Transportation, State, and Defense to review the information and determine if it can be used as the basis for judgments or should simply be reported. . . . FAA envisions that the interagency panel will make initial notifications or recommendations via the President's Council on Y2K Conversion International Working Group during the September to October 1999 timeframe. . . .

Actions taken and planned by FAA are reasonable, and satisfactorily address our recommendation.

If I can answer any questions or be of further assistance, please feel free to contact me at (202) 366-1959, or my Deputy, Raymond J. DeCarli, at (202) 366-6767.

Sincerely,

A handwritten signature in black ink, appearing to read 'K. Mead', written in a cursive style.

Kenneth M. Mead
Inspector General

Enclosure

cc: Deputy Secretary of Transportation
FAA Administrator

Enclosure



U.S. Department
of Transportation
**Federal Aviation
Administration**

Memorandum

Subject: **ACTION:** The Year 2000 Technology Challenge,
Department of Transportation, Report Number:
FE-1999-082

Date: MAY 5 1999

From: Director of the FAA Year 2000 Program Office,
AOA-4

Reply to
Attn. of:

To: Inspector General

The Federal Aviation Administration (FAA) Administrator, Jane Garvey, has asked me to respond to the Office of Inspector General's (OIG) recommendations in the subject OIG audit report.

OIG Recommendation number 1:

Take action to require key components of the aviation industry, such as passenger and cargo carriers, to provide certification of Year 2000 (Y2K) compliance no later than November 1, 1999, or such earlier date that FAA deems appropriate.

FAA Response:

Nonconcur. Requiring Y2K certification by the industry would not improve the FAA's position to take enforcement action against Y2K-related incidents. If an industry component is not Y2K compliant by January 1, 2000, the FAA's current regulatory authority is more than sufficient to take enforcement action and effectively deal with Y2K-related contingencies or emergencies. Furthermore, the relevant FAA lines of business have been surveying their industry components for Y2K status, and have assurances that most entities currently are, or will be, Y2K compliant before the end of 1999. Accordingly, the actions already being taken by the FAA fulfill the purpose of an industry certification. Three FAA lines of business provided the following specific information:

Civil Aviation Security (ACS):

Throughout calendar year 1998, ACS collected information from 459 U.S. airports as to their current readiness and preparations for the Year 2000 changeover. This inquiry focused on airport access control and allied systems that are computer-assisted, including personnel and vehicle identification systems. The results were: 109 reported that they are Y2K compliant; 109 reported that they have Y2K plans in place and are working towards being compliant; and 241 reported that they have no security systems or procedures that

are dependent on a computerized ID system. Those airports that are not Y2K compliant are working with contractors to be compliant no later than June 1999. Presently, FAA security specialists are contacting all 218 airports that have Y2K-dependant systems for a status update.

The FAA also contacted all passenger and baggage screening equipment manufacturers. All screening equipment used in U.S. airports is either Y2K compliant, or does not depend on date manipulation for the equipment to function.

In the unlikely event that a security system fails due to a Y2K problem, alternative (manual) systems to authorize and control access to restricted areas of an airport will be implemented. These procedures are outlined in Federal Aviation Regulations (FAR) 107 and 108, and the attendant Air Carrier Standard Security Program (ACSSP) and Airport Security Program (ASP). The Administrator may, under current authority, modify the ASP and ACSSP on an emergency or "for comment" basis should the need arise.

Airports (ARP):

The FAA issues airport operating certificates to 566 civil airports in the United States, which includes all airports receiving scheduled airline service. Some of the airport operator's computer systems are used in support of the safe operation of aircraft and are regulated by the FAA under 14 Code of Federal Regulations (CFR) Part 139. Part 139 covers, for example, airport rescue and fire-fighting capability, emergency response plans, airfield marking and lighting, and other requirements related to the safe operation of aircraft at the airport. The FAA is monitoring the Y2K status of these airfield systems at all of the 566 certificated airports, and is conducting site visits at the top 150 airports in the U.S. (These 150 airports serve approximately 93% of the scheduled passengers in the U.S).

The FAA plans to use its authority for the regulation of airfield safety to maintain the current level of safety at certificated airports on January 1, 2000, and beyond. The airport operator is responsible for renovating or replacing its computer systems to be Y2K compliant by January 1, 2000. If an airport does not appear to be making sufficient progress in renovating its airfield computer systems, or developing alternative means of complying with Part 139, the FAA will send those airports compliance warning letters, with a 14-day period for correction. For each airport that has not satisfactorily corrected the condition identified, the FAA will take one of the following actions:

- If the system will affect the safety or efficiency of airfield operations:
 - Issue an emergency suspension of the airport's Part 139 operating certificate, effective January 1; or
 - Issue a Notice to Airmen (NOTAM), advising that the Y2K-affected system or subsystems at the airport are unreliable and considered not available, effective January 2.

- If the system will not affect safety or have a significant effect on efficiency of airfield operations:
 - Take non-emergency enforcement action for violation of Part 139, which could include notice of proposed civil penalty, notice of proposed suspension of certificate, or administrative action.

Regulation and Certification (AVR):

AVR is working closely with U.S. certificate holders to increase awareness on their part that if they experience Y2K errors, the result could be regulatory non-compliance. It is the certificate holder's responsibility to ensure its continued compliance with safety regulations. AVR has been emphasizing to its U.S. certificate holders that they must be able to demonstrate "regulatory compliance" with operations and maintenance requirements on and after January 1, 2000. For example, an existing Flight Standards Information Bulletin (FSIB) requests U.S. certificate holders to send a letter to their Principal Inspector stating that the company and its outsource contractors will be able to show regulatory compliance with operations and maintenance requirements on and after January 1, 2000.

Readiness and Contingency Analysis Program

The FAA's Flight Standards Service (AFS), as part of its responsibility to ensure safe flight operations by U.S. certificate holders, has implemented a Readiness and Contingency Analysis Program (RCAP). This program was instituted to gather comprehensive data on the Y2K readiness of certificate holders, and provides increased awareness of potential Y2K-related problems that may impact certificate holders' regulatory compliance.

In April 1999, the RCAP office sent questionnaires to approximately 12,000 certificate holders requesting data on their Y2K readiness. It is anticipated that preliminary results from the survey will be available later in May 1999. Also, as part of the RCAP effort, a Flight Standards Information Bulletin (FSIB) is being developed which will provide guidance to inspectors on Y2K efforts. This FSIB will include RCAP program objectives; will report readiness status from the data gathered from certificate holders; will provide procedures for certificate holders to perform verification of Y2K issues and provide guidance in resolving those issues; and will establish reporting requirements for inspectors.

Manufacturers

Regarding airframe manufacturers and the Y2K issue, AVR has stated that major manufacturers are aware of the Y2K challenge and are actively preparing for it. Major airframe manufacturers have not identified any safety of flight issues with respect to Y2K issues. AVR Directorates have recently sent letters to all U.S. production approval holders and type design holders, requesting them to perform a self-assessment of both

their airborne digital products and of the tools used in the production and manufacture of airborne products. Domestically, there has been a 95 percent response rate. Responses indicate three stages of progress: (1) the manufacturer has completed the Y2K self-assessment, (2) the manufacturer has a process in place for the Y2K self-assessment and (3) the manufacturer has discovered issues (no safety of flight issues) and is addressing them.

The FAA has also developed criteria to add to the manufacturers' current inspection process - Aircraft Certification System Evaluation Program (ACSEP). AVR has made ACSEP part of its routine surveillance by both engineers and inspectors. The results of the inspections and the self-assessments will be compared. If there is an inconsistency between the self-assessment and FAA inspections, and that inconsistency could have a safety impact, FAA will perform a special site visit (to include both engineering and inspection personnel) to investigate the source of the inconsistency. If the FAA determines that there could be a safety impact as a result of the investigation, then the FAA has full statutory and regulatory authority to require whatever corrective actions are necessary.

OIG Recommendation Number 2:

The FAA should develop a policy as to whether U.S. carriers, or U.S. code flights, cargo and passengers, will be allowed to fly to countries for which there is not a credible base for concluding their air traffic control systems are Y2K compliant.

FAA Response:

Concur. The FAA is currently developing an interagency process by which the FAA will address international Y2K readiness of foreign air traffic service providers, airports and foreign flagged air carriers. FAA policy will be based upon the expected outcome of the process described below and will be focused on continued safety of the flying public.

The safety of international operations by U.S. air carriers will continue to be ensured through the normal process under which FAA-regulated carriers evaluate all factors affecting the safety of any operation. Y2K problems will be evaluated as one factor in the overall decision process of an air carrier for determining whether each and every operation can be safely conducted.

The FAA has been working with the International Civil Aviation Authority (ICAO) and other key international aviation community leaders, including the International Air Transport Association (IATA), to develop Y2K assessment criteria. These criteria can be used individually by ICAO member States to not only assess its own compliance status, but also to assess the compliance status of other States based on available information.

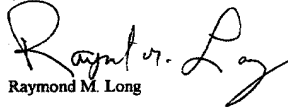
International carriers have access to the information that is presently being gathered by IATA on the status of international airports and air traffic service providers. Also, ICAO is requiring each of its member States to provide its Y2K compliance status by July 1, 1999. ICAO has also agreed to collect and publish this compliance status data from its

member States. Details of this effort are still being developed. The ICAO target is for a series of reports to be issued beginning July 15, 1999.

FAA has also proposed an interagency effort to evaluate all available international civil aviation Y2K readiness information, including the ICAO self reports. The information evaluated will consist largely of self-assessments and reports from third parties.

The FAA plans to convene an evaluation panel, comprised of representatives from FAA and the Departments of Transportation, State and Defense to review the information and determine if it can be used as the basis for judgments or should simply be reported. If the information proves to be credible, the FAA envisions that the interagency panel will make initial notifications or recommendations via the President's Council on Y2K Conversion International Working Group during the September to October 1999 time frame, with follow-up activities through December 31, 1999.

If I can be of further assistance, please contact the FAA Y2K Program Office at (202) 267-9512.



Raymond M. Long

Mrs. MORELLA. Are you finding that they are having—I mean transit systems, not just Metro, and I am going to specifically ask you about what our Metro here in Washington is doing in terms of its compliance, but in general are these public transit systems encountering problems with funding because they get some of it from States and localities?

Mr. DOWNEY. Having been in the public transit business most of my life, I would say public transit systems are always having problems with funding, but in this case most of them have put the Y2K compliance issue at the top of their list. We helped in that respect by giving clear guidance that any and all Federal funds that they receive may be used for this purpose, simplifying the process to get planning approvals, and also giving approval for simplified procurement where it was needed to use the funds effectively.

We don't think that that should be a problem. We think getting focused on it, working through the issue of how their rail equipment or bus equipment may differ from anybody else's bus or rail equipment, it is what they have to do. The large transit agencies around the country I think are working very hard at this. They are all in town this week. Both the Administrator and I will be speaking with them this afternoon, and this will be on my list in terms of what we expect them to be doing.

Mrs. MORELLA. You tell them that Congress feels the same way, too, and the Washington—I mean the Nation's Capital system should be a leader. Are they a leader?

Mr. DOWNEY. They are a leader in working on this.

Mrs. MORELLA. I just want to—I want to thank you from my point of view for answering so honestly, not only answering our questions and being here, but the work that you have done preparatory to that and how all along you have worked so very well with Congress. We wish you well.

And Mr. Chairman, I would like to ask unanimous consent that Mr. Barcia, the ranking member of the Technology Subcommittee, that his statement and statements of any other members of our two subcommittees be included in the record.

Mr. HORN. Without objection, they will be put after Mr. Turner at the beginning of the hearing record.

I want to thank all of the four witnesses. You have been very helpful to us.

First I want to thank, before I close this, the staff that put this hearing together: J. Russell George, the staff director and chief counsel in the corner down there, of the Subcommittee on Government Management, Information, and Technology; Matt Ryan, the senior policy director specifically responsible for this hearing, right behind me; Bonnie Heald, professional staff member, director of communications, immensely helpful; Mason Alinger, our clerk who has been very helpful. And for Mrs. Morella's Subcommittee on Technology of the House Science Committee, Jeff Grove, the staff director on Technology, we thank him and Joe Sullivan, the clerk, and Ben Wu, the professional staff member. And our friends on the other side of the aisle, Faith Weiss, the counsel, and Jean Gosa, the clerk, and Mike Quear, the professional staff member, and Marty Ralston, the clerk, have worked and done a very helpful job. And we thank our court reporters, as usual, Doreen Dotzler and

Laurie Harris. It takes a lot of people to prepare the hearing and permit us to have questions that are so interesting to you.

Let me now thank those that are here, and say that I think this testimony of yours has been very compelling, and it has shown that Transportation and the Federal Aviation Administration will continue to be industrious and vigilant in order to solve this problem, and we appreciate that burst of energy that will be needed to get around the course and win the game.

The Department of Transportation and the FAA provide vital services to our country. Our citizens and our economy depend on the safe and expedient transportation of both personal and business travel, goods and services, and I am concerned we have a lot of work to do. I have got a lot of faith in the people before us, that it will be done, and that you'll need the continued collaboration of Departmental officials, the airline industry, the airports themselves to ensure that the system is ready by January 1, 2000.

I appreciate the Secretary's and the Administrator's reinvigorated leadership to solve some of these technology challenges, and I think a lot of work still remains to satisfy all of us. And we will know, won't we, on January 1st when you are flying and I am flying? Just don't bump into my plane when we go across America. And I have told you, before be very nice to the controllers for the week before we board those planes.

And our oversight activities will continue on this agency as well as all others. Later in the week we are going to hear from the Federal Aviation Administration's other hat and our other hat, the financial management practices, which have nothing to do with Y2K except "Where's the money?" as somebody said, and can you put a balance sheet out. So Mr. Willemssen will be back and we will be back.

So I thank you all for your helpfulness on this, and we wish you well in the months ahead. With that, the hearing is adjourned.

[Whereupon, at 11:40 a.m., the subcommittees were adjourned.]

